(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003年10月30日 (30.10.2003)

PCT

(10) 国際公開番号
WO 03/090137 A1

(51) 国際特許分類[7]: G06F 17/60

(21) 国際出願番号: PCT/JP03/04719

(22) 国際出願日: 2003年4月14日 (14.04.2003)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2002-118411 2002年4月19日 (19.04.2002) JP

(71) 出願人 (米国を除く全ての指定国について): オムロン株式会社 (OMRON CORPORATION) [JP/JP]; 〒600-8530 京都府 京都市 下京区塩小路通堀川東入南不動堂町８０１番地 Kyoto (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 金山 憲司 (KANAYAMA,Kenji) [JP/JP]; 〒600-8530 京都府 京都市 下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内 Kyoto (JP). 鈴木 俊宏 (SUZUKI,Toshihiro) [JP/JP]; 〒600-8530 京都府 京都市 下京区塩小路通堀川東入南不動堂町８０１番地 オムロン株式会社内 Kyoto (JP).

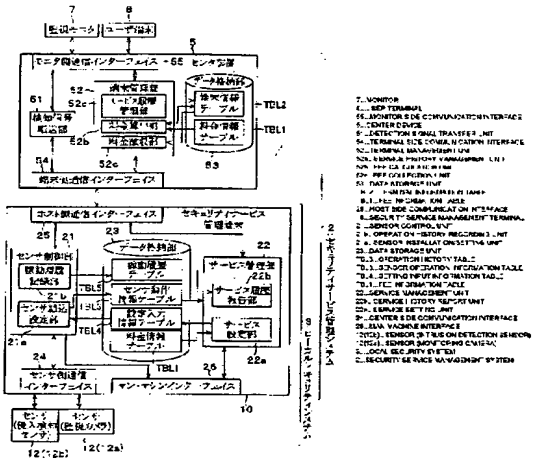
(74) 代理人: 原 謙三 (HARA,Kenzo); 〒530-0041 大阪府 大阪市 北区天神橋２丁目北２番６号 大和南森町ビル 原謙三国際特許事務所 Osaka (JP).

(81) 指定国 (国内): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL,

[続葉有]

(54) Title: SECURITY SERVICE MANAGEMENT SYSTEM, SECURITY SERVICE MANAGEMENT TERMINAL, SECURITY SERVICE MANAGEMENT METHOD, SECURITY SERVICE MANAGEMENT PROGRAM, AND COMPUTER-READABLE RECORDING MEDIUM CONTAINING THE PROGRAM

(54) 発明の名称: セキュリティサービス管理システム、セキュリティサービス管理端末、セキュリティサービス管理方法、セキュリティサービス管理プログラムならびにそれを記録したコンピュータ読み取り可能な記録媒体



(57) Abstract: A security service management system includes a security service management terminal and a center device. The security service management terminal has a sensor control unit for transmitting a detection signal acquired from a sensor to a monitor and a user terminal, an operation history recording unit for recording an operation history of the sensor, and a service history report unit for transmitting the operation history to the center device. The center device has a fee calculator for calculating a fee based on the operation history of the sensor received from the security service management terminal. Thus, it is possible to demand a fee corresponding to a service used by a user.

[続葉有]

WO 03/090137 A1

TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (広域): ARIPO 特許 (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ特許 (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI 特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各PCTガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(57) 要約: セキュリティサービス管理システムは、セキュリティサービス管理端末およびセンタ装置を備える。セキュリティサービス管理端末は、センサから取得した検知信号を監視モニタやユーザ端末へ送信するセンサ制御部と、センサの稼働履歴を記録する稼働履歴記録部と、稼働履歴をセンタ装置へ送信するサービス履歴報告部とを具備する。センタ装置は、セキュリティサービス管理端末より受信したセンサの稼働履歴に基づいて料金を算出する料金算出部を具備する。これにより、ユーザが利用したサービスの分だけの料金を請求することができる。

明　細　書

セキュリティサービス管理システム、セキュリティサービス管理端末、セキュリティサービス管理方法、セキュリティサービス管理プログラムならびにそれを記録したコンピュータ読み取り可能な記録媒体

技術分野

本発明は、ホームセキュリティ等のセキュリティサービスを提供するセキュリティサービス管理システム、セキュリティサービス管理端末、セキュリティサービス管理方法、セキュリティサービス管理プログラムならびにそれを記録したコンピュータ読み取り可能な記録媒体に関するものである。

背景技術

従来、一戸建て家屋やマンションあるいは小規模店舗を対象にしたホームセキュリティサービスがある。従来のホームセキュリティサービスでは、監視対象場所に監視カメラや侵入検知センサ等のセンサを配置し、異常な検知信号を検知すると、警備員を派遣する。そして、これらのサービスを受ける警備モードと、ユーザが家にいる時の非警備モードとを、ユーザが切り換えることができるように、センサをＯＮ／ＯＦＦできるようになっている。なお、料金体系は月単位の定額制であり、非警備モードの時間が長くても料金は変わらないのが通常である。

しかし、現在のところホームセキュリティサービスは普及が進んでいない。その一因としては、これまでのセキュリティサービスは企業等を

対象にしたものが大多数を占めており、企業向けのセキュリティサービスと同じ態勢でホームセキュリティサービスを提供しようとしてきたことにあると推測される。具体的には、従来のホームセキュリティサービスは、契約期間が長く、装置が大がかりであるため料金も高く、そのうえ装置の設置にも時間を要していた。

一方、核家族で子供が小さい間だけ、親が留守の間だけ、海外旅行中だけなどのように、「短期間だけホームセキュリティサービスを受けたい」というニーズは、今後増えてくるものと予測されている。そのため、これらニーズにこたえられる、ユーザが必要なときだけ、簡単に装置が取り付けられてすぐ利用できる、新しいホームセキュリティサービスの実現が望まれている。

しかしながら、これまでのセキュリティサービスは、企業等を対象にしたものであったため、料金も長期間契約を前提にしており、短期間の利用でユーザが利用したサービスの分だけの料金を請求することができなかった。すなわち、従来のホームセキュリティシステムでは、従量制の課金体系によってホームセキュリティサービスを提供することができなかった。

発明の開示

本発明は、上記の問題点を解決するためになされたものであり、その目的は、ホームセキュリティ等のセキュリティサービスを、オンデマンドかつ従量課金体系により提供することができるセキュリティサービス管理システム、セキュリティサービス管理端末、セキュリティサービス管理方法を提供することにある。また、本発明の目的には、上記セキュ

リティサービス管理システムを実現するセキュリティサービス管理プログラム、およびこれを記録したコンピュータ読み取り可能な記録媒体を提供することも含まれる。

上記の課題を解決するために、本発明のセキュリティサービス管理方法は、センサから検知信号を取得してモニタ装置へ送信するセンサ制御処理と、上記センサの稼働履歴を記録する履歴記録処理と、上記稼働履歴に基づいて料金を算出する料金算出処理と、を含む方法である。

上記の方法により、セキュリティサービスで使用したセンサの稼働履歴に基づいて、セキュリティサービスの料金を算出できる。よって、ユーザに対して、ユーザがセキュリティサービスを利用した分だけの料金を請求することが可能となる。ここで、料金算出のベースとなるセンサの稼動履歴としては、センサが実際に稼動した時間の情報や送信した画像の枚数の情報等を、単独であるいは組み合わせて利用できる。したがって、上記セキュリティサービス管理方法によれば、ホームセキュリティ等のセキュリティサービスを、従量課金体系により提供することが可能となる。

また、本発明のセキュリティサービス管理システムは、セキュリティサービス管理端末およびセンタ装置を備えたセキュリティサービス管理システムであって、上記セキュリティサービス管理端末は、センサから取得した検知信号をモニタ装置へ送信するセンサ制御部と、上記センサの稼働履歴を記録する稼働履歴記録部と、上記稼働履歴を上記センタ装置へ送信するサービス履歴報告部とを具備し、上記センタ装置は、上記セキュリティサービス管理端末より受信した上記センサの稼働履歴に基づいて料金を算出する料金算出部を具備する構成である。

上記の構成により、セキュリティサービスで使用したセンサの稼働履歴に基づいて、セキュリティサービスの料金を算出できる。よって、ユーザに対して、ユーザがセキュリティサービスを利用した分だけの料金を請求することが可能となる。ここで、料金算出のベースとなるセンサの稼動履歴としては、センサが実際に稼動した時間の情報や送信した画像の枚数の情報等を、単独であるいは組み合わせて利用できる。したがって、上記セキュリティサービス管理システムによれば、ホームセキュリティ等のセキュリティサービスを、従量課金体系により提供することが可能となる。

また、本発明のセキュリティサービス管理端末は、センサから取得した検知信号をモニタ装置へ送信するセンサ制御部と、上記センサの稼働履歴を記録する稼働履歴記録部と、上記稼働履歴記録部によって記録された稼働履歴を、当該稼働履歴に基づいて料金を算出する料金算出部を備えたセンタ装置へ送信するサービス履歴報告部と、を具備する構成である。

上記の構成により、セキュリティサービスで使用したセキュリティサービス管理端末に接続されたセンサの稼働履歴に基づき、センタ装置においてセキュリティサービスの料金を算出できる。よって、ユーザに対して、ユーザがセキュリティサービスを利用した分だけの料金を請求することが可能となる。ここで、料金算出のベースとなるセンサの稼動履歴としては、センサが実際に稼動した時間の情報や送信した画像の枚数の情報等を、単独であるいは組み合わせて利用できる。したがって、上記セキュリティサービス管理端末によれば、ホームセキュリティ等のセキュリティサービスを、従量課金体系により提供することが可能となる

また、本発明のセキュリティサービス管理端末は、センサから取得した検知信号をモニタ装置へ送信するセンサ制御部と、上記センサの稼働履歴を記録する稼働履歴記録部と、上記稼働履歴に基づいて料金を算出する料金算出部と、料金徴収装置とを具備するとともに、上記料金算出部が算出した料金を上記料金徴収装置により徴収する料金徴収部を具備する構成である。

上記の構成により、さらに、適当な料金徴収装置を利用して、プリペイドカード、電子マネー、現金、クレジットカード等によって料金を徴収できる。したがって、上記セキュリティサービス管理端末によれば、センサからの検知信号の取得および送信の機能に加えて、料金の算出および徴収の機能を一装置に実現することが可能となる。その結果、セキュリティサービスを提供する現場において効率的に料金を徴収することが可能となる。

本発明のさらに他の目的、特徴、および優れた点は、以下に示す記載によって十分わかるであろう。また、本発明の利益は、添付図面を参照した次の説明で明白になるであろう。

図面の簡単な説明

図１は、本発明の一実施の形態に係るセキュリティサービス管理システムの構成の概略を示す機能ブロック図である。

図２は、図１に示したセキュリティサービス管理システムが管理するセキュリティシステムの概略を示す説明図である。

図３は、図１に示したセキュリティサービス管理システムによるセキ

ュリティサービスにおける課金方法を示す説明図である。

図４は、図１に示したセキュリティサービス管理システムの料金情報テーブルの一例を示す説明図である。

図５は、図１に示したセキュリティサービス管理システムの端末情報テーブルの一例を示す説明図である。

図６は、図１に示したセキュリティサービス管理システムのセンサ動作情報テーブルの一例を示す説明図である。

図７は、図１に示したセキュリティサービス管理システムの設定入力情報テーブルの一例を示す説明図である。

図８は、図１に示したセキュリティサービス管理システムの起動時の処理を示すフローチャートである。

図９は、図１に示したセキュリティサービス管理システムの警備モードの処理を示すフローチャートである。

図１０は、図１に示したセキュリティサービス管理システムの課金処理を示すフローチャートである。

図１１は、図１に示したセキュリティサービス管理端末において設定入力時に表示される画面例を示す説明図である。

図１２は、図１に示したセキュリティサービス管理システムの変形例の構成の概略を示す機能ブロック図である。

図１３は、図１２に示したセキュリティサービス管理端末において設定入力時に表示される画面例を示す説明図である。

発明を実施するための最良の形態

本発明の一実施の形態について図１から図１３に基づいて説明すれば

、以下のとおりである。なお、図１は、センタ装置５で料金を算出し徴収する構成例であり、図１２は、セキュリティサービス管理端末１０で料金を算出し徴収する構成例である。

本実施の形態に係るセキュリティサービス管理システム２（図２）は、ユーザがサービスを受けたい時間帯やセンサの種類および数を随時設定でき、サービスを受けた時間分だけ課金されるホームセキュリティ等のセキュリティサービスを提供する。そのために、セキュリティサービス管理システム２では、利用履歴（稼働履歴テーブルＴＢＬ５，端末情報テーブルＴＢＬ２）を記録し、それに応じて料金を算出する。これにより、短期契約（例えば、一日から数日）でのセキュリティサービスの提供が実現できる。

例えば、図３に示すように、セキュリティサービス管理システム２は、実際にセキュリティ監視を実行した時間を積算して、これをベースに利用料金を算出する。次の数式（１）は、料金の計算式の一例である。なお、数式（１）の演算で使用する具体的な金額や係数等は、料金情報テーブルＴＢＬ１（図４）にあらかじめ設定されている。また、数式（１）は、係数等の追加により適宜変更可能である。以下、本実施の形態では、数式（１）に従って料金を算出する場合について説明するが、サービス形態により料金の算出式が適宜設定可能であることはいうまでもない。

$$\text{料金} = \text{契約種別} \times \sum_{i=1}^{n} [\{\text{警備パターン別単価} + (\text{センサ単価} \times \text{センサ個数}) + (\text{カメラ単価} \times \text{カメラ個数})\} \times \text{サービス利用時間} ti] \quad \cdots (1)$$

ここで、「警備パターン」とは、例えば、センサが検知した検知信号

をユーザに送信するのみ（警備パターン１）、検知信号をユーザが確認後、ユーザの要求に応じて警備員を派遣する（警備パターン２）、警備会社が検知信号を確認し、異常の内容により必要であれば警備員を派遣する全面的な委託（警備パターン３）の別である。そして、「警備パターン別単価」とは、警備パターンごとにあらかじめ設定された単位時間あたりの料金である。

また、「契約種別」とは、例えば、単一期間契約、複数期間契約、常時契約の別である。そして、数式（１）において、「契約種別」はあらかじめ設定された係数として演算される。なお、この係数は、すべての警備パターンに共通に設定されている。

また、「センサ単価」および「カメラ単価」とは、あらかじめ設定されたセンサ／カメラの単位時間あたりの料金である。これらの単価は、すべての警備パターンに共通に設定しても、警備パターンごとに設定してもよい。また、「センサ個数」および「カメラ個数」とは、契約期間に含まれる警備期間ｔ1～ｔnの各警備期間ごとに使用されたセンサ／カメラの個数である。

そして、図３に示すように、単一期間契約の場合、警備期間ｔnの前に機器を設置し、警備期間ｔnの後に機器を撤去する契約であり、警備モードがオンされた警備期間ｔnのみに課金する。また、複数期間契約の場合、警備期間ｔ1の前に機器を設置し、警備期間ｔ2の後に機器を撤去する契約であり、警備モードがオンされた警備期間ｔ1およびｔ2のみに課金する。常時契約の場合、機器の撤去時期を定めない契約であり、警備モードがオンされた警備期間ｔ1～ｔnのみに課金する。なお、複数期間契約あるいは常時契約の場合、契約期間に含まれる警備期間ｔ1～

ｔｎの各警備期間ごとに、警備パターンやセンサおよびカメラの個数が異なってもよい。

このように、セキュリティサービス管理システム２は、実際にセキュリティ監視を実行した時間（サービス利用時間）に応じて、利用料金を算出できる。なお、監視カメラのように映像を検知するセンサの場合、送信した映像（静止画）の枚数をベースに利用料金を算出してもよい。また、センサおよびカメラは一度設置したら、それらのすべてをいずれの警備期間でも使用する場合、すなわち、センサおよびカメラの種類および数が警備期間ごとに変更されない場合には、サービス利用時間を警備パターンごとに積算するようにして、利用料金の算出式を簡単化できる。

また、セキュリティサービス管理システム２は、サービス開始までの作業（セキュリティ機器の取り付けやシステムへの各種情報の設定等）をユーザが行う自己設定型のタイム・セキュリティサービスを提供する。そのために、セキュリティサービス管理システム２では、カメラなどのセンサがプラグ・アンド・プレイで動作する。すなわち、ユーザがセンサをセキュリティサービス管理端末１０に接続して電源を投入すると、自動的にセンサがシステムへ組み込まれ利用可能となる。これにより、利用申し込みからサービス開始までのすべての作業をユーザが自分で行うことができる。

以上により、セキュリティサービス管理システム２では、ホームセキュリティサービスを、オンデマンドかつ従量課金体系により提供することができる。また、料金の徴収をプリペイドカードを使った料金前払いで行うこともできる。また、セキュリティ機器のレンタルも可能となる

図２に示すように、セキュリティシステム１は、センタ装置５に、ローカルセキュリティシステム３が公衆網４を介して、監視モニタ（モニタ装置）７やユーザ端末（モニタ装置）８がインターネット網６を介して、それぞれ接続されて構成されている。

センタ装置５は、セキュリティシステム１によるセキュリティサービスを提供するセキュリティサービス会社等に設置された、セキュリティサービス全体を管理する装置である。センタ装置５には、複数の監視対象場所に設置されたローカルセキュリティシステム３…が、公衆網４を介して接続されている。公衆網４としては、電話網、携帯電話網、パケット通信網、ＰＨＳ（personal handyphone system）等が利用できる。

監視対象場所であるユーザの家屋や小規模店舗等の監視対象場所には、ローカルセキュリティシステム３が設置されている。ローカルセキュリティシステム３では、監視カメラや侵入検知センサ等のセンサ１２…を各所に配置し、検知した検知信号をセキュリティサービス管理端末１０が収集して、監視モニタ７やユーザ端末８へ送信する。

なお、ローカルセキュリティシステム３のセキュリティサービス管理端末１０と、センタ装置５が、公衆網４を介して相互通信可能に接続されて、セキュリティサービス管理システム２が構成されている。また、センタ装置５、セキュリティサービス管理端末１０、センサ１２…には、ＩＰ（internet protocol）アドレスが割り当てられている。

ここで、ローカルセキュリティシステム３のゲートウェイであるセキュリティサービス管理端末１０は、例えば、ＣＰＵと、メモリと、外部

装置とのインターフェイスとを搭載した１チップコンピュータに、ＬＣＤ（liquid crystal display）等の表示装置と、キーパッド等の入力装置とを接続することで構成できる。このように、セキュリティサービス管理端末１０は、非常に簡単な構成の装置として実現できるため、小型かつ安価であり、しかも据え付けおよび動作設定が容易である。

なお、本実施の形態では、セキュリティサービス管理システム２の基本的な機能、すなわち、センサの検知信号を転送する機能および料金を算出する機能を中心に説明するが、さらに高度な機能を設ける場合には、センタ装置５に設けることが好ましい。これにより、ローカルセキュリティシステム３には簡易な装置を設置しながらも、セキュリティサービス管理システム２全体では高度な機能が実現できる。もちろん、セキュリティサービス管理システム２のシステム構成は、センタ装置５に機能を集中させた集中処理型に限定されず、セキュリティサービス管理端末１０により多くの機能を分担させた分散処理型の構成も可能である。そして、いずれの機能をセキュリティサービス管理端末１０に行わせるかは、セキュリティサービス管理システム２の要求仕様に応じて適宜選択できる。

監視モニタ７は、警備員派遣会社に設けられた監視設備である。この警備員派遣会社は、監視モニタ７で異常を知らせる検知信号を受信したり、ユーザ等から警備員の派遣依頼を受信した時、監視対象場所であるユーザの家屋等に警備員を派遣する。

ユーザ端末８は、監視計画の設定入力、監視状況の確認、センサの制御、料金の見積や請求の確認などをユーザが行うことができるように、あらかじめ情報の送信先として設定された装置である。ユーザ端末８と

しては、ユーザが常時携帯している携帯電話等が利用できる。

このように、セキュリティサービス管理端末１０は、広域の通信ネットワークである公衆網４およびインターネット網６を介して、セキュリティサービス会社のセンタ装置５、警備員派遣会社の監視モニタ７、ユーザのユーザ端末８に接続されている。このような構成とすることによって、警備員やユーザは、ローカルセキュリティシステム３のセキュリティサービス管理端末１０から送信されてくる情報によって、各センサ１２によるセンシング状況を把握することが可能となり、例えば留守中の警備などが可能となる。

図１は、セキュリティサービス管理システム２、すなわちローカルセキュリティシステム３およびセンタ装置５の一構成（センタ装置５で料金を算出し徴収する構成例）の概略を示す機能ブロック図である。

図１に示すように、ローカルセキュリティシステム３は、セキュリティサービス管理端末１０に、センサ１２が主としてワイヤレスによるセンサネット１１を介して通信可能に接続されて構成されている。

センサ１２は、監視対象の異常を検知し、検知結果を検知信号として出力する。センサ１２は、通常、特定の目的、例えば屋内侵入監視、火災監視、子供や病人あるいはペットの監視、車両盗難監視等の目的に応じて選択され、その目的に応じた適切な場所に設置される。このようなセンサの一例を挙げると、次のとおりである。

人体等を検知するものとしては、光電センサ、ビームセンサ、超音波センサ、赤外線センサ等がある。物体の動きや破壊等を検知するものとしては、振動センサ、加速度センサ（３Ｄセンサ）等がある。音を検知するものとしては、マイクロホン、音感センサ、音響センサ等がある。

映像を検知するものとしては、ビデオカメラ等がある。火災等を検知するものとしては、温度センサ、煙センサ、湿度センサ等がある。人や車両等の移動するものに装着されるものとしては、ＧＰＳ（global positioning system）、加速度センサ、ワイパＯＮ／ＯＦＦセンサ、振動センサ、傾斜センサ等がある。室内に設置されるものとしては、照明ＯＮ／ＯＦＦセンサ、水漏れセンサ等がある。屋外に設置されるものとしては、雨量計、風速計、温度計等がある。これら以外にも、静電容量レベルセンサ、静電容量浸入センサ、電流センサ、電圧センサ、ドアの開閉を検知するリードスイッチ、時刻を検知する時計等、多種多様なものがある。

このように、センサ１２は、一般に「センサ」と呼ばれるものに限られておらず、現象を検知してその検知結果を電気信号に変換するなどして検知信号を出力することができるあらゆる機器を含んでいる。

また、センサ１２は、監視カメラであってもよい。監視カメラは、撮像管、ＣＣＤ（charge coupled device）撮像素子あるいはＣＭＯＳ（complementary metal oxide semiconductor（相補型金属酸化膜半導体））撮像素子などによって構成される撮像部以外に、ズーム機能やオートフォーカス機能等を備え、自動的に、あるいはセキュリティサービス管理端末１０からの制御信号により動作可能なものをいう。なお、セキュリティサービス管理端末１０は、センタ装置５、監視モニタ７、ユーザ端末８から要求に基づいて、制御信号を発生することもできる。このような能動型センサでは、現象に応じてより的確な検知を行うことができる。

さらに、センサ１２は自律型センサであってもよい。ここでは、自律

型センサとは、そのセンサ自身に関する情報（センサ情報）ならびに検知結果を、セキュリティサービス管理端末１０に対して、例えば周期的に報知するものをいう。センサ情報とは、例えばそのセンサの種類（検知できる内容等を含む）および配置（位置、設置場所）の情報である。

センサは車両等の移動体に取り付けられる場合もある。センサが移動すると、そのセンサでの検知結果により得られる情報は変化し得る。例えば、センサとして車両に取り付けられた温度計を考えると、そのセンサで気温を検知する場合、車両の位置、つまりセンサの位置によって検知結果がどの地点での気温を表しているかが異なることになる。このような場合に自律型センサを用いると、常にどの地点での気温を検知しているかを認識することができる。

図１では、センサ１２の一例として、監視カメラであるセンサ１２ａ、赤外線を利用した侵入検知センサであるセンサ１２ｂを示している。なお、この例はあくまで一例であり、センサ１２としては、上記した各種センサのどれを用いても構わない。また、図１には、ローカルセキュリティシステム３にセンサ１２ａおよびセンサ１２ｂを設けた構成しか示していないが、実際にはさらに多数のセンサ１２が設けられていても構わない。

また、センサ１２は、後述するように、プラグ・アンド・プレイにより、セキュリティサービス管理端末１０に接続することができる。

次に、セキュリティサービス管理端末１０は、ローカルセキュリティシステム３においてセキュリティサービスの全体を統括管理する。セキュリティサービス管理端末１０は、特に、センサ１２が取得した情報を外部の監視モニタ７やユーザ端末８へ送信する機能（センサのマスタユ

ニットとしての機能）、および、ユーザが利用したセキュリティサービスに対して課金を行う機能を備えている。

具体的には、図１に示すように、セキュリティサービス管理端末１０は、センサ制御部（センサ制御手段）２１、サービス管理部２２、データ格納部２３、センサ側通信インターフェイス２４、ホスト側通信インターフェイス２５、マン・マシンインターフェイス２６を備えて構成されている。

センサ制御部２１は、センサ１２において検知された検知信号を無線通信ネットワークであるセンサネット１１を介して受信するとともに、この検知信号をセンタ装置５を介して外部の監視モニタ７やユーザ端末８へ送信する。特に、センサ制御部２１は、異常発生時に監視モニタ７やユーザ端末８へ警報を発動する。なお、センサ制御部２１は、センサ１２から取得した検知信号を、センタ装置５を介さずに、監視モニタ７やユーザ端末８へ直接送信してもよい。

また、センサ制御部２１は、設定入力情報テーブルＴＢＬ４（図７）に設定されている稼働計画に従ってセンサ１２の稼動させる。また、センサ制御部２１は、センタ装置５、監視モニタ７、ユーザ端末８からの指示に従って、センサ１２を制御することもできる。

また、センサ制御部２１は、センサ１２から受信した検知結果を保存する。具体的には、稼働履歴記録部（履歴記録手段）２１ｂが、センサ１２の稼働履歴をリアルタイムで稼働履歴テーブルＴＢＬ５に記録する。

さらに、センサ制御部２１は、センサ１２をプラグ・アンド・プレイによりセキュリティサービス管理端末１０およびセンタ装置５（すなわ

ち、セキュリティサービス管理システム２）にセットアップするセンサ組込設定部２１ａを備えている。センサ組込設定部２１ａは、センサ１２からＩＤコードを受信することでプラグ・アンド・プレイを確立する。

ここで、図８を参照しながら、セキュリティサービス管理システム２の起動動作の概略を説明する。特に、センサ１２を、プラグ・アンド・プレイにより、セキュリティサービス管理端末１０に組み込む動作を説明する。

図８に示すように、ユーザがセキュリティサービス管理端末１０を設置し電源を投入すると（Ｓ１１１）、セキュリティサービス管理端末１０は自動で立ち上がり、ユーザからのコマンド入力待ちおよびセンサやカメラからのセンサ立ち上がり通知待ちに入る（Ｓ１１２）。

また、ユーザが監視カメラ１２ａや侵入検知センサ１２ｂを設置し電源を投入すると（Ｓ１２１）、監視カメラ１２ａや侵入検知センサ１２ｂは自動で立ち上がり、セキュリティサービス管理端末１０へ「立ち上がり通知」を送信する。

セキュリティサービス管理端末１０は、監視カメラ１２ａや侵入検知センサ１２ｂからの「立ち上がり通知」を受信すると「応答」を返し、これを監視カメラ１２ａや侵入検知センサ１２ｂが検出すると、自分のＩＤコードや動作状態を送信する（Ｓ１２２）。なお、センサ１２のＩＤコードは、センサ種別、個体別（同じセンサでもＩＤコードは別）に設定されている。また、センサ機器をレンタルする場合、レンタル業者がＩＤコードを設定できる。

セキュリティサービス管理端末１０は、センサ１２から受信（Ｓ１１

３）したＩＤコード等の情報をもとに、センサ動作情報テーブルＴＢＬ３（図６）を自動的に作成する（Ｓ１１４）。セキュリティサービス管理端末１０は、ステップＳ１１２～Ｓ１１４の処理を繰り返し、すべてのセンサ１２をセンサ動作情報テーブルＴＢＬ３に登録すると（Ｓ１１５）、その旨を表示し、ユーザの確認を待つ（Ｓ１１６）。

次に、セキュリティサービス管理端末１０は、ユーザが確認ＯＫを入力すると（Ｓ１３１）、センタ装置５にダイアルアップ等によって接続して、「初期設定要求」を送信する（Ｓ１１７）。

一方、センタ装置５は、電源投入（Ｓ１０１）の後、セキュリティ監視センタシステムとしての各種動作を実行する（Ｓ１０２）。そして、セキュリティサービス管理端末１０から「初期設定要求」を受信すると（Ｓ１０３）、「応答」を返し、これをセキュリティサービス管理端末１０が検出すると 「初期設定情報」を送信する（Ｓ１１８）。

センタ装置５は受信した初期設定情報をもとに、セキュリティ監視センタとして必要な端末情報テーブルＴＢＬ２（図５）を作成し（Ｓ１０５）、セキュリティサービス管理端末１０をセキュリティシステム１に組み込む。

また、センサ１２のステップＳ１２１，１２２の処理、およびセキュリティサービス管理端末１０のステップＳ１１２～Ｓ１１８の処理は、センサ１２が接続された時点で常に実行される。すなわち、センサ組込設定部２１ａは、センサ１２がセキュリティサービス管理端末１０に接続された時、そのセンサ１２をセンサ動作情報テーブルＴＢＬ３に登録するとともに、センタ装置５へ通知する。そして、センタ装置５は、この通知に基づき端末情報テーブルＴＢＬ２を設定する。

このように、セキュリティサービス管理端末１０およびセンサ１２がプラグ・アンド・プレイでセキュリティシステム１に組み込まれるため、ローカルセキュリティシステム３の機器の取付をユーザに行わせることが可能となる。その結果、機器の取付時の作業を省力化できるとともに、ユーザが機器を取り付けた時点から、直ちにその機器を利用したセキュリティサービスを提供することができる。具体的には、センタ装置５がセンサ１２…を個別に管理できるため、センタ装置５が関与するセキュリティサービスを高度化することが可能となる。例えば、監視カメラ１２ａが撮影した画像データの管理や、監視カメラ１２ａの制御を、センタ装置５において行うことができる。

つづいて、サービス管理部２２は、サービス設定部２２ａおよびサービス履歴報告部２２ｂを備えている。

サービス設定部（稼働計画設定手段）２２ａは、センサ１２の稼働計画を設定し、設定入力情報テーブルＴＢＬ４（図７）に記録する。具体的には、サービス設定部２２ａは、セキュリティサービスを受ける警備モードと、ユーザが家にいる時などにセキュリティサービスを停止する非警備モードとを、ユーザが切り換えることができるように、センサ１２をＯＮ／ＯＦＦする予定を設定できる。この設定は、センサ１２ごとに行うことができる。もちろん、ユーザの設定後、直ちに警備モードをオンすることも可能である。なお、センサ１２の状態は、センサ組込設定部２１ａにより逐次取得され、センサ動作情報テーブル３ＴＢＬ３に反映される。

また、サービス設定部（料金見積手段）２２ａは、ユーザがマン・マシンインターフェイス２６を用いて稼働計画を設定する際、入力値（サ

ービス利用時間（見積りの時点では警備期間に等しい）、警備パターン、センサ個数）に応じた見積料金を算出して提示する（図１１）。これにより、ユーザは、セキュリティサービスの利用をあらかじめシミュレートして、料金を確認できる。なお、サービス設定部２２ａからは、契約の変更などのセンサ１２の稼働計画以外の変更も可能である。

サービス履歴報告部（サービス履歴報告手段）２２ｂは、稼働履歴記録部２１ｂが記録した稼働履歴テーブルＴＢＬ５に基づいて、センサ１２の稼働履歴をセンタ装置５へ送信する。この送信は、例えば、警備期間の終了時点、すなわち警備モードをオフする時点で行う。

センサ側通信インターフェイス２４は、例えばＲＦ（radio frequency）信号による無線通信を行う。このセンサ側通信インターフェイス２４によって、センサ制御部２１は、センサネット１１を介して、センサ１２と双方向データ通信が可能となる。ここでの無線通信の方式としては、例えば特定小電力無線通信システムや無線ＬＡＮなどが挙げられるが、その他、無線による通信が可能な方式であればどのようなものを用いてもよい。例えば、ＩＥＥＥ８０２．１１に準拠する無線ＬＡＮや、Ｂｌｕｅｔｏｏｔｈ（登録商標）などを用いたネットワークとすることも可能である。

ホスト側通信インターフェイス２５は、公衆網４、具体的には、電話網、携帯電話網、パケット通信網、ＰＨＳとの通信インターフェイス機器である。

マン・マシンインターフェイス２６は、キーボードやタッチパネル等の入力機器、およびＬＣＤ（liquid crystal display）等の出力機器である。

データ格納部２３は、料金情報テーブルＴＢＬ１、機器動作情報テーブルＴＢＬ３、設定入力情報テーブルＴＢＬ４、稼動履歴テーブルＴＢＬ５を格納している。

図４に示すように、料金情報テーブルＴＢＬ１には、後述するセンタ装置５の料金算出部５２ｂ（図１）やセキュリティサービス管理端末１０′の料金算出部２２ｃ（図１２）等において、例えば上述した数式（１）に従って料金を算出する際に使用する具体的な単価・係数等があらかじめ設定されている。

図６に示すように、機器動作情報テーブルＴＢＬ３には、セキュリティサービス管理端末１０に接続されている各センサ１２の「ＩＤコード」、「接続状態」、「動作状態」が設定される。ここで、ＩＤコードとは、セキュリティサービス管理システム２で統一的に使用される管理符号である。接続状態とは、セキュリティサービス管理端末２に動作可能に設定されているか否かを示す。動作状態とは、センサ１２のオン／オフの状態を示す。

図７に示すように、設定入力情報テーブルＴＢＬ４には、センサ１２の稼動計画であり、警備サービスの予定として、「開始時刻」、「終了時刻」、「警備パターン」、「使用センサ」が設定される。ここで、警備パターンには、例えば上述したようなサービス内容を指定する警備パターン１～３のいずれかが設定される。使用センサには、警備に使用するセンサ１２のＩＤコードが設定される。

また、図１に示すように、センタ装置５は、検知信号転送部５１、端末管理部５２、データ格納部５３、端末側通信インターフェイス５４、モニタ側通信インターフェイス５５を備えて構成されている。

検知信号転送部５１は、センサ１２の検知信号をセンサ制御部２１より受信して、外部の監視モニタ７やユーザ端末８へ送信する。また、検知信号転送部５１は、監視モニタ７やユーザ端末８からセンサ１２に対する制御要求を受信して、センサ制御部２１へ送信する。

端末管理部５２は、セキュリティサービスに関するデータをセキュリティサービス管理端末１０ごとに管理する。端末管理部５２は、サービス履歴管理部５２ａ、料金算出部５２ｂ、料金徴収部５２ｃを備えている。

サービス履歴管理部５２ａは、警備期間ごとにサービス履歴報告部２２ｂから受信するセンサ１２の稼働履歴に基づいて、端末情報テーブルＴＢＬ２（図５）を更新する。

料金算出部（料金算出手段）５２ｂは、サービス履歴管理部５２ａが端末情報テーブルＴＢＬ２に記録したセンサ１２の稼働履歴のデータに基づき、料金情報テーブルＴＢＬ１を参照して、料金を算出し、端末情報テーブルＴＢＬ２に記録する。なお、セキュリティサービス管理端末１０やユーザ端末８に見積料金を提示する場合、稼働計画をセンタ装置５に送信して、料金算出部５２ｂに見積額を算出させ、結果を取得して提示してもよい。

料金徴収部５２ｃは、料金算出部５２ｂが端末情報テーブルＴＢＬ２に記録した未精算の料金を、クレジットカード、プリペイドカード、電子マネー、現金等により徴収する処理を行う。

例えば、料金徴収部５２ｃは、ユーザへの請求書の送信／送付を行う。また、後述するような料金徴収装置２７（図１２）をセキュリティサービス管理端末１０に設けて、料金徴収部５２ｃからの指示に基づき、

料金をセキュリティサービス管理端末１０において徴収してもよい。なお、この場合であっても、料金算出部５２ｂおよび料金徴収部５２ｃがセンタ装置５に設けられているため、料金を統一的に把握・管理できるとともに、高いセキュリティを確保して不正使用等を防止できる。

データ格納部５３は、料金情報テーブルＴＢＬ１および端末情報テーブルＴＢＬ２を格納している。なお、料金情報テーブルＴＢＬ１（図４）は、セキュリティサービス管理端末１０のデータ格納部２３に格納されているものと同一である。

図５に示すように、端末情報テーブルＴＢＬ２には、警備モードの「開始時刻」、「終了時刻」、「警備パターン」、使用された「センサ個数」、「カメラ個数」、「サービス利用時間」、「基本料金」、「契約」の係数、「総計」が設定される。サービス利用時間は、セキュリティサービスの利用時間であり、開始時刻と終了時刻から求められる。基本料金は、数式（１）で契約種別の係数をかける前の金額である。総計は、端末情報テーブルＴＢＬ２ごとの未清算の料金である。なお、端末情報テーブルＴＢＬ２は、ユーザ等の要求に応じて、端末管理部５２によりユーザ端末８に、あるいはい、サービス管理部２２によりマン・マシンインターフェイス２６に提示される。

端末側通信インターフェイス５４は、公衆網４、具体的には、電話網、携帯電話網、パケット通信網、ＰＨＳとの通信インターフェイス機器である。

モニタ側通信インターフェイス５５は、インターネット網６との通信インターフェイス機器である。

上述のように、セキュリティサービス管理システム２では、数式（１）に従ってサービス利用時間をベースに料金を算出するために、センサ１２の稼働履歴（警備の開始時刻および終了時刻、警備パターン、センサ個数、カメラ個数）を、稼働履歴記録部２１ｂ、サービス履歴報告部２２ｂ、サービス履歴管理部５２ａの順で転送する。また、センサ１２の状態はセンサ動作情報テーブルＴＢＬ３から取得できる。また、サービス設定部２２ａが、契約種別を契約更改時にサービス履歴管理部５２ａへ別途送信する。よって、セキュリティサービス管理システム２は、実際にセキュリティ監視を実行した時間に応じて、利用料金を算出できる。

ここで、上記セキュリティサービス管理端末１０（１０′（図１３））は、汎用のコンピュータをベースに構成できる。また、上記センタ装置５（５′（図１３））は、ワークステーションやパーソナルコンピュータ等の汎用のコンピュータをベースに構成できる。すなわち、上記のセキュリティサービス管理端末１０（１０′）およびセンタ装置５（５′）は、それぞれの機能を実現するプログラム（セキュリティサービス管理プログラム）の命令を実行するＣＰＵ（centralprocessing unit）、ブートロジックを格納したＲＯＭ（read only memory）、上記プログラムを展開するＲＡＭ（random access memory）、上記プログラムおよび各種データを格納するハードディスク等の記憶装置（記録媒体）、キーボード、マウス、タッチパネル等の入力機器、モニタやスピーカー等の出力機器、他の機器と通信する通信機器などを備えている。そして、上記情報配信プログラムは、フロッピィー（登録商標）ディスク、ハードディスク、磁気テープ、ＣＤ－ＲＯＭ／光ディスク／光磁気デ

ィスク／ＭＤなどのメディア、およびＲＯＭ／ＲＡＭメモリなどの記録媒体にコンピュータで読み取り可能に記録されている。

つづいて、図９から図１２を参照しながら、セキュリティシステム１の動作について説明する。

図９は、セキュリティシステム１の警備モードにおける処理を示すフローチャートである。

侵入検知センサ１２ｂは、設定入力情報テーブルＴＢＬ４（図７）に基づくセンサ制御部２１の制御によって、警備開始時刻になると待機状態から警備モードに遷移し、セキュリティ監視を実行する（Ｓ２０１）。そして、侵入検知センサ１２ｂは、常時監視状態にあり異常を検出すると、センサ制御部２１に検知信号を送出して監視カメラ１２ａの動作開始を要請する。

侵入検知センサ１２ｂから監視カメラ１２ａの動作開始要請を受信（Ｓ２１１）したセンサ制御部２１は、監視カメラ１２ａに対してカメラ撮像指令を送出する（Ｓ２１２）。この指令に応じて、監視カメラ１２ａはカメラ撮影を開始し撮影したカメラ画像を送出する。そして、センサ制御部２１は、監視カメラ１２ａおよび侵入検知センサ１２ｂから受信したカメラ画像およびセンサ情報をセンタ装置５へ送信する（Ｓ２１３）。

次に、センタ装置５では、センサ制御部２１から受信したカメラ画像・センサ情報を蓄積する（Ｓ２２２）とともに、ユーザの設定した警備パターン情報に基づき、所定の警備パターン動作を行う。

具体的には、警備パターン１，２であれば（Ｓ２２２でＮＯ）、ユーザのユーザ端末８である携帯端末／電話に対して異常通知とカメラ画像

送信を行い（Ｓ２１４）、これらの情報を確認したユーザから警備員派遣要請があった場合は（Ｓ２３１，Ｓ２３２）、警備員を派遣する（Ｓ２４３）。また、警備パターン３であれば（Ｓ２２２でＹＥＳ）、警備員派遣会社の監視モニタ７に対して異常通知とカメラ画像送信を行い（Ｓ２２３）、これらの情報を確認したオペレータが警備員派遣を決定した場合（Ｓ２４１，Ｓ２４２）、警備員を派遣する（Ｓ２４３）。

なお、ステップＳ２３２において、稼働計画で警備パターン１が設定されている場合であっても、ユーザが警備員の派遣を希望する時は、その時点で警備パターン２に切り換えてもよいし、警備開始後の警備パターンの変更は認めないが、オプションのサービスとして警備員の派遣を行ってもよい。

図１０は、セキュリティサービス管理端末１０およびセンタ装置５の処理を示すフローチャートである。

まず、ユーザが、監視対象局所にローカルセキュリティシステム３を構成する各種セキュリティ機器（セキュリティサービス管理端末１０、監視カメラ１２ａ、侵入検知センサ１２ｂ）を据え付ける。そして、ユーザが、マン・マシンインターフェイス２６から「警備の開始時刻」、「警備の終了時刻」、「警備パターン」等の設定を入力する（Ｓ３０１）。

サービス設定部２２ａがユーザの入力した設定入力情報を受付けると（Ｓ３１１）、センサ組込設定部２１ａがセンサ１２の状態を確認してセンサ動作情報テーブルＴＢＬ３を作成し、センサ１２の接続／動作状態をマン・マシンインターフェイス２６に表示する（Ｓ３１２）。この表示に基づいて、ユーザが使用可能なセンサの中から警備に使用する「

センサ」、「カメラ」等を選択する。そして、ユーザが、警備計画（センサの稼働計画）の内容を確認する（Ｓ３０２）。このとき、マン・マシンインターフェイス２６には、サービス設定部２２ａが料金情報テーブルＴＢＬ１を参照して算出した見積料金が表示される。（図１１）また、警備計画は複数の警備期間を一時に設定できる。

ユーザが設定入力を確認し、「ＯＫ」を入力すると、サービス設定部２２ａは、ユーザが入力した設定入力情報に基づき、設定入力情報テーブルＴＢＬ４を作成し（Ｓ３１３）、これをセンタ装置５のサービス履歴管理部５２ａへ送信する（Ｓ３１４）。そして、サービス履歴管理部５２ａは、サービス履歴報告部２２ｂから送られてきた設定入力情報テーブルＴＢＬ４の情報をベースに、端末情報テーブルＴＢＬ２等のシステムとして必要な各種テーブルを自動作成する（Ｓ３３１）。

セキュリティサービス管理端末１０は、設定入力情報テーブルＴＢＬ４を設定した後、警備モードの待機状態（警備モードオフ）に遷移する。そして、最初の警備期間ｔ1の警備開始時刻になると（Ｓ３１５）、センサ制御部２１がセンサ１２を稼働させるとともに、稼働履歴記録部２１ｂが履歴の記録を開始する（Ｓ３１６）。その後、設定された警備終了時刻になると（Ｓ３１７）、センサ制御部２１がセンサ１２を停止させるとともに、サービス履歴報告部２２ｂがセンサ１２の稼働履歴を稼働履歴テーブルＴＢＬ５から読み出して、サービス履歴管理部５２ａへ送信する（Ｓ３１８）。そして、セキュリティサービス管理端末１０は、次の警備期間の開始時刻を読み出し、待機状態に遷移する（Ｓ３２０）。セキュリティサービス管理端末１０は、この警備モードのオン／オフの動作（Ｓ３１５～Ｓ３１８）を、センサ動作情報テーブルＴＢＬ

３に設定されているすべての警備期間ｔｉ（ｉ＝１～ｎ）が終了するまで繰り返す（Ｓ３１９）。

一方、センタ装置５では、サービス履歴管理部５２ａがステップ３３１で作成した端末情報テーブルＴＢＬ２を、サービス履歴報告部２２ｂから履歴報告を受信するたびに更新する（Ｓ３３２）。そして、更新のたびに、料金算出部５２ｂが、数式（１）に従って履歴をベースに契約種別を考慮して料金計算を行う（Ｓ３３３）。さらに、料金徴収部５２ｃが、適当なタイミングでユーザに料金請求を行い（Ｓ３３４）、ユーザによる料金支払いを受ける（Ｓ３０３）。なお、料金徴収部５２ｃが、料金請求するタイミングは、計画されているすべての警備期間が終了した時点でもよいし、１、２回ごとや、所定単位期間ごとであってもよい。

なお、ユーザが警備計画の変更指示を行えば、いつでもステップＳ３１２にもどって、設定入力情報テーブルＴＢＬ４を変更できる。また、サービス設定部２２ａは、契約の満了日が近づくと、機器撤去の予定をマン・マシンインターフェイス２６に表示する。

ここで、図１１は、ユーザが警備計画を作成する際に、セキュリティサービス管理端末１０のマン・マシンインターフェイス２６に表示される表示画面例である。

図１１に示すように、設定入力情報テーブルＴＢＬ４を作成するために必要な「開始時刻」、「終了時刻」、「警備パターン」が入力可能に表示される。また、「センサ個数」、「カメラ個数」には、ユーザがセンサ／カメラの選択画面（図示せず）で選択したセンサ／カメラの個数が表示される。そして、使用する監視カメラ１２ａの映像がモニタ画像

として表示される。さらに、「開始時刻」および「終了時刻」から警備期間が計算されて表示され、この警備期間と他の設定入力情報とに基づき、料金情報テーブルＴＢＬ１を参照して算出した見積料金が表示される。

上記のように、セキュリティサービス管理システム２では、サービス開始までの作業をユーザによる作業として、センタ装置５の対応を無人化することにより、従来システムに比較して大幅な時間短縮とコスト削減を実現できる。また、履歴に基づいて課金するため、従来のサービスでは不可能であった細かな料金設定にもとづく時間単位のセキュリティサービスが実現できる。

また、図１２は、セキュリティサービス管理システム２の他の構成（セキュリティサービス管理端末１０で料金を算出し徴収する構成例）の概略を示す機能ブロック図である。以下では、図１と相違する点のみ説明する。

図１２に示すように、セキュリティサービス管理端末１０′は、セキュリティサービス管理端末１０と比べて、料金徴収装置２７が設けられており、サービス管理部２２に、料金算出部２２ｃおよび料金徴収部２２ｄが追加されている。また、センタ装置５′は、センタ装置５と比べて、端末管理部５２から料金算出部５２ｂおよび料金徴収部５２ｃ、データ格納部５３から料金情報テーブルＴＢＬ１がそれぞれ省略されている。

料金算出部（料金算出手段）２２ｃは、料金算出部５２ｂ（図１）とほぼ同じ処理を行う。具体的には、料金算出部２２ｃは、稼働履歴テーブルＴＢＬ５から読み出したセンサ１２の稼働履歴に基づいて料金を算

出する。これにより、ユーザが利用したサービスの分だけの料金を請求することができる。

料金徴収部（料金徴収手段）２２ｄは、料金算出部２２ｃが算出した料金を料金徴収装置２７により徴収する。セキュリティサービス管理端末１０′では、料金徴収装置２７としてプリペイドカード装置を搭載している。なお、料金徴収装置２７を選択することにより、プリペイドカードの他、ＩＣカード、電子マネーや現金等による徴収も可能である。

セキュリティサービス管理端末１０′およびセンタ装置５′の動作は、図１０で説明した動作とほぼ同じである。異なる点としては、まず、ステップＳ３０１において、料金徴収部２２ｄが料金徴収装置２７に挿入されているプリペイドカードの残りカウントを読み取る。また、ステップＳ３０３において、料金徴収部２２ｄが料金徴収装置２７に挿入されているプリペイドカードから料金相当分のカウントを減算する。

さらに、料金徴収部２２ｄは、プリペイドカードの残りカウントを適当なタイミングで随時確認し、不足を検知するとプリペイドカードの追加を求めるメッセージをマン・マシンインターフェイス２６に表示する。このメッセージは、ユーザ端末８にも提示してもよい。なお、プリペイドカードのカウントが無くなり、追加を要求しても新たなプリペイドカードが追加されない場合、警備を直ちに中止することも可能であるし、警備を続行して割増料金を請求することも可能ではある。

ここで、図１３は、ユーザが警備計画を作成する際に、セキュリティサービス管理端末１０′のマン・マシンインターフェイス２６に表示される表示画面例である。

図１３に示すように、セキュリティサービス管理端末１０′での表示

３に設定されているすべての警備期間ｔｉ（ｉ＝１～ｎ）が終了するまで繰り返す（Ｓ３１９）。

一方、センタ装置５では、サービス履歴管理部５２ａがステップ３３１で作成した端末情報テーブルＴＢＬ２を、サービス履歴報告部２２ｂから履歴報告を受信するたびに更新する（Ｓ３３２）。そして、更新のたびに、料金算出部５２ｂが、数式（１）に従って履歴をベースに契約種別を考慮して料金計算を行う（Ｓ３３３）。さらに、料金徴収部５２ｃが、適当なタイミングでユーザに料金請求を行い（Ｓ３３４）、ユーザによる料金支払いを受ける（Ｓ３０３）。なお、料金徴収部５２ｃが、料金請求するタイミングは、計画されているすべての警備期間が終了した時点でもよいし、１、２回ごとや、所定単位期間ごとであってもよい。

なお、ユーザが警備計画の変更指示を行えば、いつでもステップＳ３１２にもどって、設定入力情報テーブルＴＢＬ４を変更できる。また、サービス設定部２２ａは、契約の満了日が近づくと、機器撤去の予定をマン・マシンインターフェイス２６に表示する。

ここで、図１１は、ユーザが警備計画を作成する際に、セキュリティサービス管理端末１０のマン・マシンインターフェイス２６に表示される表示画面例である。

図１１に示すように、設定入力情報テーブルＴＢＬ４を作成するために必要な「開始時刻」、「終了時刻」、「警備パターン」が入力可能に表示される。また、「センサ個数」、「カメラ個数」には、ユーザがセンサ／カメラの選択画面（図示せず）で選択したセンサ／カメラの個数が表示される。そして、使用する監視カメラ１２ａの映像がモニタ画像

として表示される。さらに、「開始時刻」および「終了時刻」から警備期間が計算されて表示され、この警備期間と他の設定入力情報とに基づき、料金情報テーブルＴＢＬ１を参照して算出した見積料金が表示される。

上記のように、セキュリティサービス管理システム２では、サービス開始までの作業をユーザによる作業として、センタ装置５の対応を無人化することにより、従来システムに比較して大幅な時間短縮とコスト削減を実現できる。また、履歴に基づいて課金するため、従来のサービスでは不可能であった細かな料金設定にもとづく時間単位のセキュリティサービスが実現できる。

また、図１２は、セキュリティサービス管理システム２の他の構成（セキュリティサービス管理端末１０で料金を算出し徴収する構成例）の概略を示す機能ブロック図である。以下では、図１と相違する点のみ説明する。

図１２に示すように、セキュリティサービス管理端末１０′は、セキュリティサービス管理端末１０と比べて、料金徴収装置２７が設けられており、サービス管理部２２に、料金算出部２２ｃおよび料金徴収部２２ｄが追加されている。また、センタ装置５′は、センタ装置５と比べて、端末管理部５２から料金算出部５２ｂおよび料金徴収部５２ｃ、データ格納部５３から料金情報テーブルＴＢＬ１がそれぞれ省略されている。

料金算出部（料金算出手段）２２ｃは、料金算出部５２ｂ（図１）とほぼ同じ処理を行う。具体的には、料金算出部２２ｃは、稼働履歴テーブルＴＢＬ５から読み出したセンサ１２の稼働履歴に基づいて料金を算

出する。これにより、ユーザが利用したサービスの分だけの料金を請求することができる。

料金徴収部（料金徴収手段）２２ｄは、料金算出部２２ｃが算出した料金を料金徴収装置２７により徴収する。セキュリティサービス管理端末１０′では、料金徴収装置２７としてプリペイドカード装置を搭載している。なお、料金徴収装置２７を選択することにより、プリペイドカードの他、ＩＣカード、電子マネーや現金等による徴収も可能である。

セキュリティサービス管理端末１０′およびセンタ装置５′の動作は、図１０で説明した動作とほぼ同じである。異なる点としては、まず、ステップＳ３０１において、料金徴収部２２ｄが料金徴収装置２７に挿入されているプリペイドカードの残りカウントを読み取る。また、ステップＳ３０３において、料金徴収部２２ｄが料金徴収装置２７に挿入されているプリペイドカードから料金相当分のカウントを減算する。

さらに、料金徴収部２２ｄは、プリペイドカードの残りカウントを適当なタイミングで随時確認し、不足を検知するとプリペイドカードの追加を求めるメッセージをマン・マシンインターフェイス２６に表示する。このメッセージは、ユーザ端末８にも提示してもよい。なお、プリペイドカードのカウントが無くなり、追加を要求しても新たなプリペイドカードが追加されない場合、警備を直ちに中止することも可能であるし、警備を続行して割増料金を請求することも可能ではある。

ここで、図１３は、ユーザが警備計画を作成する際に、セキュリティサービス管理端末１０′のマン・マシンインターフェイス２６に表示される表示画面例である。

図１３に示すように、セキュリティサービス管理端末１０′での表示

は、図１１に示した表示画面例とほぼ同一である。異なる点としては、「現在の残りカウント」が表示されることと、見積料金とともに見積料金に相当するカウント数が表示されることである。

このように、セキュリティサービス管理端末１０′によれば、これまでのセキュリティサービスで実現されていなかったプリペイドカードによる料金徴収が実現できる。よって、ユーザがプリペイドカードをスーパー等で手軽に購入できる一方、セキュリティサービス会社は前金による商売が可能となる。

また、プリペイドカードの残りカウント数を取得する際、そのカードに記録されている他の情報を読み取って、セキュリティサービスに利用することもできる。

また、セキュリティサービス管理端末１０′に料金徴収装置２７を設けず、料金徴収部２２ｄがクレジットカード会社等のコンピュータに直接アクセスして、ユーザのカードから支払いを受けるように手続きしてもよい。そしてさらに、センサ制御部２１が、監視モニタ７あるいはユーザ端末８へ直接、検知信号を送信すれば、センタ装置５を省略できる。

なお、本発明のセキュリティサービス管理方法は、センサから検知信号を取得してモニタ装置へ送信するセンサ制御処理と、上記センサの稼働履歴を記録する履歴記録処理と、上記稼働履歴に基づいて料金を算出する料金算出処理と、を含む方法であってもよい。

上記の方法により、セキュリティサービスで使用したセンサの稼働履歴に基づいて、セキュリティサービスの料金を算出できる。よって、ユーザに対して、ユーザがセキュリティサービスを利用した分だけの料金

を請求することが可能となる。ここで、料金算出のベースとなるセンサの稼動履歴としては、センサが実際に稼動した時間の情報や送信した画像の枚数の情報等を、単独であるいは組み合わせて利用できる。したがって、上記セキュリティサービス管理方法によれば、ホームセキュリティ等のセキュリティサービスを、従量課金体系により提供することが可能となる。

さらに、本発明のセキュリティサービス管理方法は、上記センサの稼働計画を設定する稼働計画設定処理をさらに含み、上記センサ制御処理において、上記稼働計画に従ってセンサを稼動させる方法であってもよい。

上記の方法により、さらに、セキュリティサービスにおいて、ユーザがあらかじめ設定した稼働計画に従ってセンサを稼動させることができる。しかも、使用したセンサの稼働履歴に基づいて、ユーザがセキュリティサービスを利用した分だけの料金を請求できるため、離散的な警備スケジュールであっても完全な従量課金が可能である。したがって、上記セキュリティサービス管理方法によれば、ホームセキュリティ等のセキュリティサービスを、オンデマンドかつ従量課金体系により提供することが可能となる。

さらに、本発明のセキュリティサービス管理方法は、上記稼働計画に基づき見積料金を算出して提示する料金見積処理を含む方法であってもよい。

上記の方法により、さらに、センサの稼働計画に基づき見積料金を提示できる。これにより、ユーザは、設定した稼動計画に従ってセキュリティサービスを受けた場合に請求される料金をあらかじめ確認した上で

、稼動計画を確定することができる。

さらに、本発明のセキュリティサービス管理方法は、上記料金算出処理において算出した料金を、料金徴収装置により徴収する料金徴収処理を含む方法であってもよい。

上記の方法により、さらに、適当な料金徴収装置を利用して、プリペイドカード、電子マネー、現金、クレジットカード等によって料金を徴収できる。したがって、上記セキュリティサービス管理方法によれば、セキュリティサービスを提供する現場においても効率的に料金を徴収することが可能となる。

また、本発明のセキュリティサービス管理システムは、セキュリティサービス管理端末およびセンタ装置を備えたセキュリティサービス管理システムであって、上記セキュリティサービス管理端末は、センサから取得した検知信号をモニタ装置へ送信するセンサ制御手段と、上記センサの稼働履歴を記録する履歴記録手段と、上記稼働履歴を上記センタ装置へ送信する履歴報告手段とを具備し、上記センタ装置は、上記セキュリティサービス管理端末より受信した上記センサの稼働履歴に基づいて料金を算出する料金算出手段を具備する構成であってもよい。

上記の構成により、セキュリティサービスで使用したセンサの稼働履歴に基づいて、セキュリティサービスの料金を算出できる。よって、ユーザに対して、ユーザがセキュリティサービスを利用した分だけの料金を請求することが可能となる。ここで、料金算出のベースとなるセンサの稼動履歴としては、センサが実際に稼動した時間の情報や送信した画像の枚数の情報等を、単独であるいは組み合わせて利用できる。したがって、上記セキュリティサービス管理システムによれば、ホームセキュ

リティ等のセキュリティサービスを、従量課金体系により提供することが可能となる。

さらに、本発明のセキュリティサービス管理システムは、上記セキュリティサービス管理端末は、上記センサの稼働計画を設定する稼働計画設定手段をさらに具備し、かつ、上記センサ制御手段が上記稼働計画に従ってセンサを稼動させるものであってもよい。

上記の構成により、さらに、セキュリティサービスにおいて、ユーザがあらかじめ設定した稼働計画に従ってセンサを稼動させることができる。しかも、使用したセンサの稼働履歴に基づいて、ユーザがセキュリティサービスを利用した分だけの料金を請求できるため、離散的な警備スケジュールであっても完全な従量課金が可能である。したがって、上記セキュリティサービス管理システムによれば、ホームセキュリティ等のセキュリティサービスを、オンデマンドかつ従量課金体系により提供することが可能となる。

さらに、本発明のセキュリティサービス管理システムは、上記セキュリティサービス管理端末は、上記稼働計画に基づく見積料金を算出して提示する料金見積手段をさらに具備する構成であってもよい。

上記の構成により、さらに、センサの稼働計画に基づき見積料金を提示できる。これにより、ユーザは、設定した稼動計画に従ってセキュリティサービスを受けた場合に請求される料金をあらかじめ確認した上で、稼動計画を確定することができる。

さらに、本発明のセキュリティサービス管理システムは、料金徴収装置を備え、上記料金算出手段が算出した料金を上記料金徴収装置により徴収する料金徴収手段を具備する構成であってもよい。

上記の構成により、さらに、適当な料金徴収装置を利用して、プリペイドカード、電子マネー、現金、クレジットカード等によって料金を徴収できる。したがって、上記セキュリティサービス管理システムによれば、セキュリティサービスを提供する現場においても効率的に料金を徴収することが可能となる。

また、本発明のセキュリティサービス管理端末は、センサから取得した検知信号をモニタ装置へ送信するセンサ制御手段と、上記センサの稼働履歴を記録する履歴記録手段と、上記履歴記録手段によって記録された稼働履歴を、当該稼働履歴に基づいて料金を算出する料金算出手段を備えたセンタ装置へ送信する履歴報告手段と、を具備する構成であってもよい。

上記の構成により、セキュリティサービスで使用したセキュリティサービス管理端末に接続されたセンサの稼働履歴に基づき、センタ装置においてセキュリティサービスの料金を算出できる。よって、ユーザに対して、ユーザがセキュリティサービスを利用した分だけの料金を請求することが可能となる。ここで、料金算出のベースとなるセンサの稼動履歴としては、センサが実際に稼動した時間の情報や送信した画像の枚数の情報等を、単独であるいは組み合わせて利用できる。したがって、上記セキュリティサービス管理端末によれば、ホームセキュリティ等のセキュリティサービスを、従量課金体系により提供することが可能となる。

さらに、本発明のセキュリティサービス管理端末は、センサから取得した検知信号をモニタ装置へ送信するセンサ制御手段と、上記センサの稼働履歴を記録する履歴記録手段と、上記稼働履歴に基づいて料金を算

出する料金算出手段と、料金徴収装置とを具備するとともに、上記料金算出手段が算出した料金を上記料金徴収装置により徴収する料金徴収手段を具備する構成であってもよい。

上記の構成により、さらに、適当な料金徴収装置を利用して、プリペイドカード、電子マネー、現金、クレジットカード等によって料金を徴収できる。したがって、上記セキュリティサービス管理端末によれば、センサからの検知信号の取得および送信の機能に加えて、料金の算出および徴収の機能を一装置に実現することが可能となる。その結果、セキュリティサービスを提供する現場において効率的に料金を徴収することが可能となる。

さらに、本発明のセキュリティサービス管理端末は、上記センサの稼働計画を設定する稼働計画設定手段をさらに具備し、上記センサ制御手段が上記稼働計画に従ってセンサを稼動させるものであってもよい。

上記の構成により、さらに、セキュリティサービスにおいて、ユーザがあらかじめ設定した稼働計画に従ってセンサを稼動させることができる。しかも、使用したセンサの稼働履歴に基づいて、ユーザがセキュリティサービスを利用した分だけの料金を請求できるため、離散的な警備スケジュールであっても完全な従量課金が可能である。したがって、上記セキュリティサービス管理端末によれば、ホームセキュリティ等のセキュリティサービスを、オンデマンドかつ従量課金体系により提供することが可能となる。

さらに、本発明のセキュリティサービス管理端末は、上記稼働計画に基づく見積料金を算出して提示する料金見積手段を具備する構成であってもよい。

上記の構成により、さらに、センサの稼働計画に基づき見積料金を提示できる。これにより、ユーザは、設定した稼動計画に従ってセキュリティサービスを受けた場合に請求される料金をあらかじめ確認した上で、稼動計画を確定することができる。

また、本発明のセキュリティサービス管理プログラムは、コンピュータを上記セキュリティサービス管理システムの各手段として機能させるコンピュータ・プログラムである。

上記の構成により、コンピュータで上記セキュリティサービス管理システムの各手段を実現することによって、上記セキュリティサービス管理システムを実現することができる。したがって、上記したセキュリティサービス管理システムの効果である、ホームセキュリティ等のセキュリティサービスを、オンデマンドかつ従量課金体系により提供できるという効果を奏する。

また、本発明のセキュリティサービス管理プログラムは、コンピュータを上記セキュリティサービス管理端末の各手段として機能させるコンピュータ・プログラムである。

上記の構成により、コンピュータで上記セキュリティサービス管理端末の各手段を実現することによって、上記セキュリティサービス管理端末を実現することができる。したがって、上記したセキュリティサービス管理端末の効果である、ホームセキュリティ等のセキュリティサービスを、オンデマンドかつ従量課金体系により提供できるという効果を奏する。

また、本発明のセキュリティサービス管理プログラムを記録したコンピュータ読み取り可能な記録媒体は、上記セキュリティサービス管理シ

ステムあるいは上記セキュリティサービス管理端末の各手段をコンピュータに実現させて、上記セキュリティサービス管理システムあるいは上記セキュリティサービス管理端末を動作させるセキュリティサービス管理プログラムを記録したコンピュータ読み取り可能な記録媒体である。

上記の構成により、上記記録媒体から読み出されたセキュリティサービス管理プログラムによって、上記セキュリティサービス管理システムあるいは上記セキュリティサービス管理端末をコンピュータ上に実現することができる。

発明の詳細な説明の項においてなされた具体的な実施態様または実施例は、あくまでも、本発明の技術内容を明らかにするものであって、そのような具体例にのみ限定して狭義に解釈されるべきものではなく、本発明の精神と特許請求事項との範囲内で、いろいろと変更して実施することができるものである。

産業上の利用の可能性

本発明に係るセキュリティサービス管理システムは、セキュリティサービスをオンデマンドかつ従量課金体系により提供することができるため、核家族で子供が小さい間だけ、親が留守の間だけ、海外旅行中だけなどのように、ユーザが必要なときだけ、簡単に装置が取り付けられてすぐ利用できるホームセキュリティサービスに好適である。

請　求　の　範　囲

１．センサから検知信号を取得してモニタ装置へ送信するセンサ制御処理と、

上記センサの稼働履歴を記録する履歴記録処理と、

上記稼働履歴に基づいて料金を算出する料金算出処理と、を含むセキュリティサービス管理方法。

２．上記センサの稼働計画を設定する稼働計画設定処理をさらに含み、

上記センサ制御処理において、上記稼働計画に従ってセンサを稼動させる請求項１に記載のセキュリティサービス管理方法。

３．上記稼働計画に基づき見積料金を算出して提示する料金見積処理を含む請求項２に記載のセキュリティサービス管理方法。

４．上記料金算出処理において算出した料金を、料金徴収装置により徴収する料金徴収処理を含む請求項１から３のいずれか１項に記載のセキュリティサービス管理方法。

５．セキュリティサービス管理端末およびセンタ装置を備えたセキュリティサービス管理システムであって、

上記セキュリティサービス管理端末は、

センサから取得した検知信号をモニタ装置へ送信するセンサ制御手段と、

上記センサの稼働履歴を記録する履歴記録手段と、

上記稼働履歴を上記センタ装置へ送信する履歴報告手段とを具備し、

上記センタ装置は、上記セキュリティサービス管理端末より受信した上記センサの稼働履歴に基づいて料金を算出する料金算出手段を具備するセキュリティサービス管理システム。

６．上記セキュリティサービス管理端末は、

上記センサの稼働計画を設定する稼働計画設定手段をさらに具備し、かつ、

上記センサ制御手段が上記稼働計画に従ってセンサを稼動させるものである請求項５に記載のセキュリティサービス管理システム。

７．上記セキュリティサービス管理端末は、

上記稼働計画に基づく見積料金を算出して提示する料金見積手段をさらに具備する請求項６に記載のセキュリティサービス管理システム。

８．料金徴収装置を備え、

上記料金算出手段が算出した料金を上記料金徴収装置により徴収する料金徴収手段を具備する請求項５から７のいずれか１項に記載のセキュリティサービス管理システム。

９．センサから取得した検知信号をモニタ装置へ送信するセンサ制御手段と、

上記センサの稼働履歴を記録する履歴記録手段と、

上記履歴記録手段によって記録された稼働履歴を、当該稼働履歴に基づいて料金を算出する料金算出手段を備えたセンタ装置へ送信する履歴報告手段と、を具備するセキュリティサービス管理端末。

１０．センサから取得した検知信号をモニタ装置へ送信するセンサ制御手段と、

上記センサの稼働履歴を記録する履歴記録手段と、

上記稼働履歴に基づいて料金を算出する料金算出手段と、

料金徴収装置とを具備するとともに、

上記料金算出手段が算出した料金を上記料金徴収装置により徴収する料金徴収手段を具備するセキュリティサービス管理端末。

１１．上記センサの稼働計画を設定する稼働計画設定手段をさらに具備し、

上記センサ制御手段が上記稼働計画に従ってセンサを稼動させるものである請求項９または１０に記載のセキュリティサービス管理端末。

１２．上記稼働計画に基づく見積料金を算出して提示する料金見積手段を具備する請求項１１に記載のセキュリティサービス管理端末。

１３．請求項５から８のいずれか１項に記載のセキュリティサービス管理システムを動作させるセキュリティサービス管理プログラムであって、コンピュータを上記の各手段として機能させるためのセキュリティサービス管理プログラム。

１４．請求項９から１２のいずれか１項に記載のセキュリティサービス管理端末を動作させるセキュリティサービス管理プログラムであって、コンピュータを上記の各手段として機能させるためのセキュリティサービス管理プログラム。

１５．請求項１３または１４に記載のセキュリティサービス管理プログラムを記録したコンピュータ読み取り可能な記録媒体。

図 1

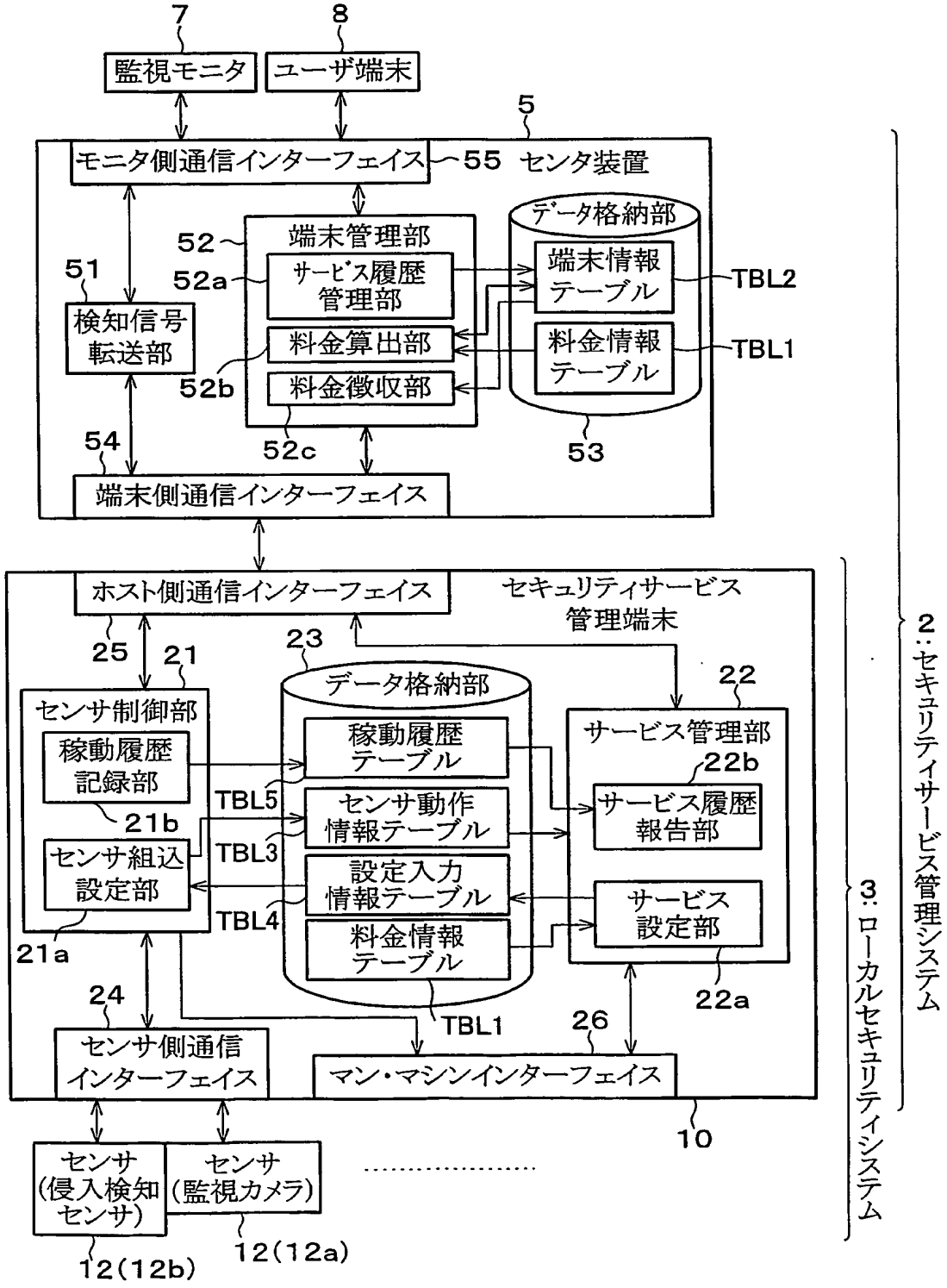

7
8
監視モニタ
ユーザ端末
5
モニタ側通信インターフェイス
55
センタ装置
データ格納部
端末管理部
52
サービス履歴管理部
52a
端末情報テーブル
TBL2
51
検知信号転送部
料金算出部
料金情報テーブル
TBL1
52b
料金徴収部
54
52c
53
端末側通信インターフェイス
ホスト側通信インターフェイス
セキュリティサービス管理端末
25
21
23
22
データ格納部
センサ制御部
稼動履歴テーブル
サービス管理部
稼動履歴記録部
22b
TBL5
センサ動作情報テーブル
サービス履歴報告部
21b
TBL3
センサ組込設定部
設定入力情報テーブル
サービス設定部
TBL4
料金情報テーブル
21a
22a
24
TBL1
26
センサ側通信インターフェイス
マン・マシンインターフェイス
10
センサ(侵入検知センサ)
センサ(監視カメラ)
12(12b)
12(12a)
2:セキュリティサービス管理システム
3:ローカルセキュリティシステム

図 2

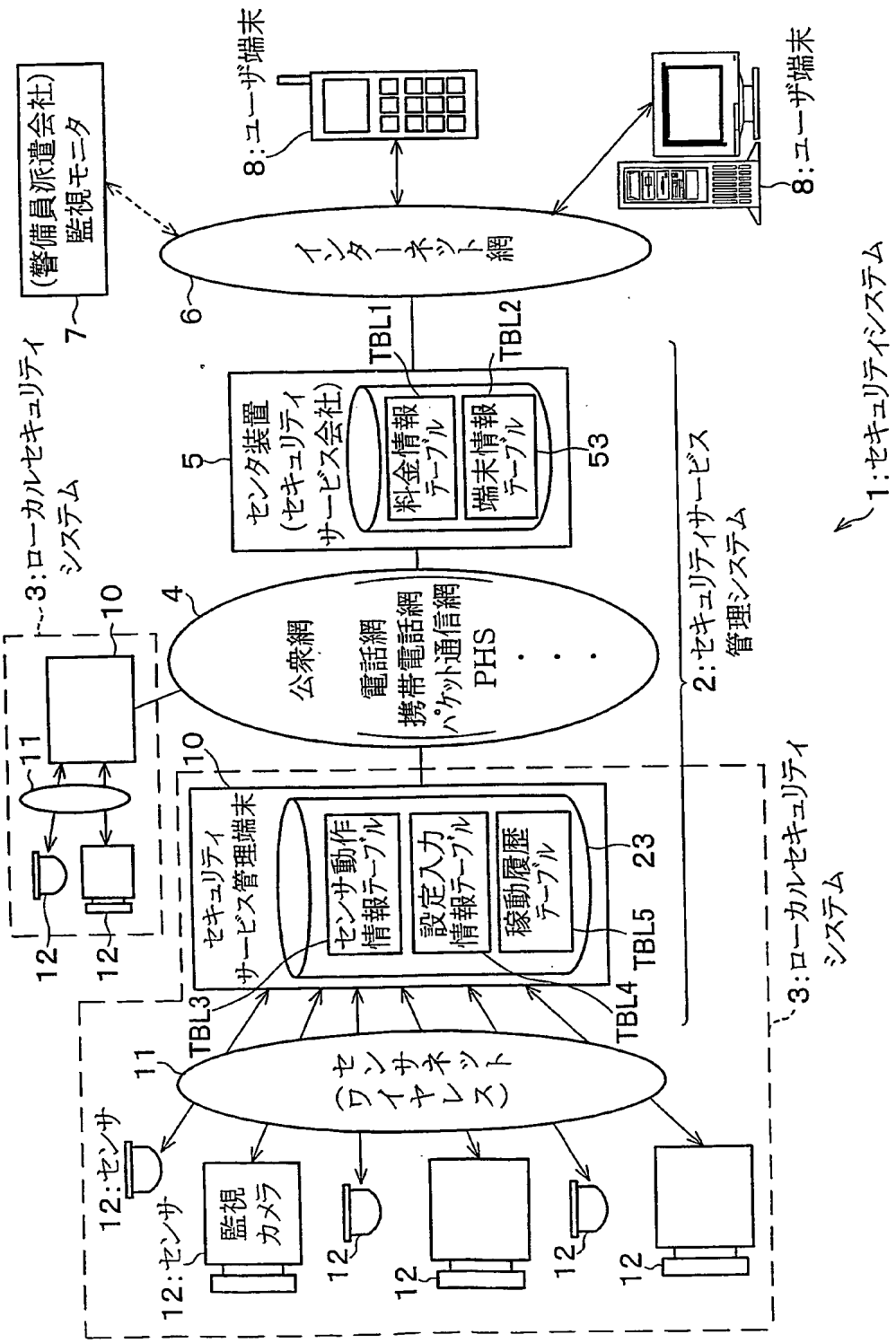

1:セキュリティシステム
2:セキュリティサービス管理システム
3:ローカルセキュリティシステム
3:ローカルセキュリティシステム
4
公衆網
電話網
携帯電話網
パケット通信網
PHS
5
センタ装置
(セキュリティサービス会社)
料金情報テーブル
端末情報テーブル
53
TBL1
TBL2
6
インターネット網
7
(警備員派遣会社)
監視モニタ
8:ユーザ端末
8:ユーザ端末
10
セキュリティサービス管理端末
センサ動作情報テーブル
設定入力情報テーブル
稼動履歴テーブル
23
TBL3
TBL4
TBL5
11
センサネットワーク
12:センサ
12:センサ
監視カメラ
12
12
12
12
12

図 3

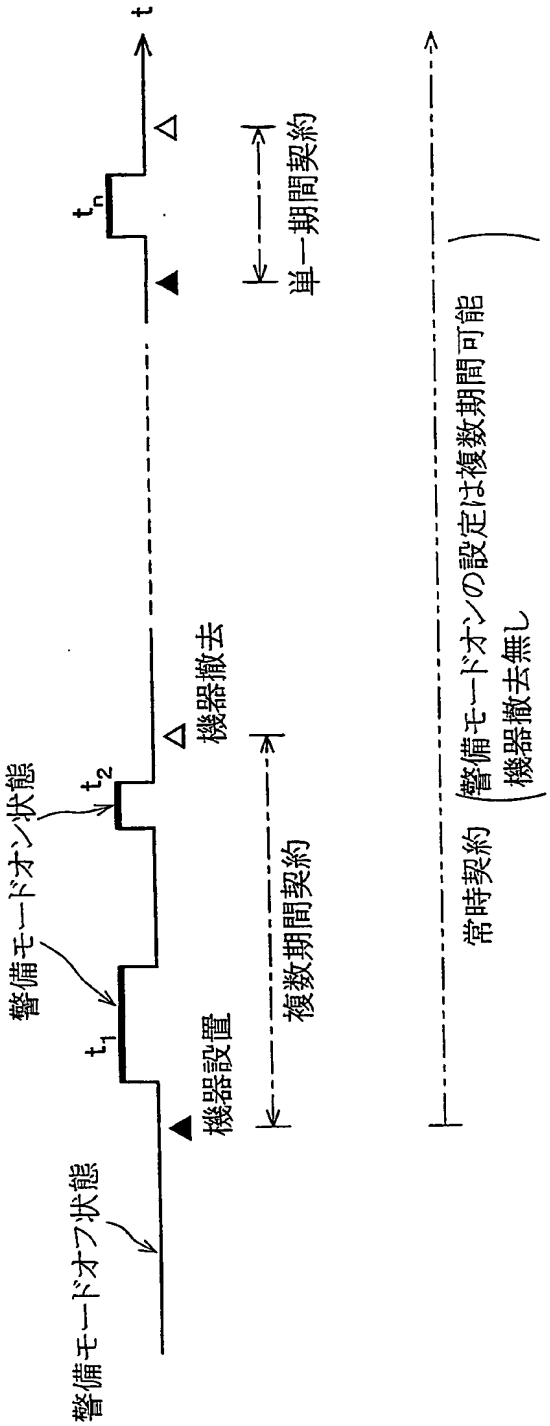

警備モードオフ状態
警備モードオン状態
機器設置
機器撤去
t
t1
t2
tn
複数期間契約
単一期間契約
常時契約
(警備モードオンの設定は複数期間可能
機器撤去無し)

図 4

料金情報テーブル

警備パターン／時間	センサ料金／個	契約(係数)
(ユーザ確認) ① 100円	(侵入検知センサ) 5円	(単一) 1.0
(ユーザ確認・警備員派遣) ② 200円	(監視カメラ) 10円	(複数) 0.9
(全面委託) ③ 300円		(常時) 0.8

TBL1

図 5

端末情報テーブル

開始時刻	終了時刻	警備パターン	センサ個数	カメラ個数	時間単価	サービス利用時間	基本料金	契約	総計
0416 2000	0416 2300	①	2	1	120	3	360	(常時) 0.8	50,976
0427 1200	0505 1200	③	2	2	330	192	63,360		
：	：	：	：	：	：	：	：		

TBL2

図 6

センサ動作情報テーブル

IDコード	接続状態	動作状態
A0001(侵入検知センサ)	接続	稼動
A0002(侵入検知センサ)	接続	稼動
B0001(監視カメラ)	接続	稼動
B0002(監視カメラ)	切断	停止
⋮	⋮	⋮

TBL3

図 7

設定入力情報テーブル

契約	開始時刻	終了時刻	警備パターン	使用センサ
常時	0416 2000	0416 2300	①	A0001 A0002 B0001
	0427 1200	0505 1200	③	A0001 A0002 B0001 B0002
	⋮	⋮	⋮	⋮

TBL4

図 8

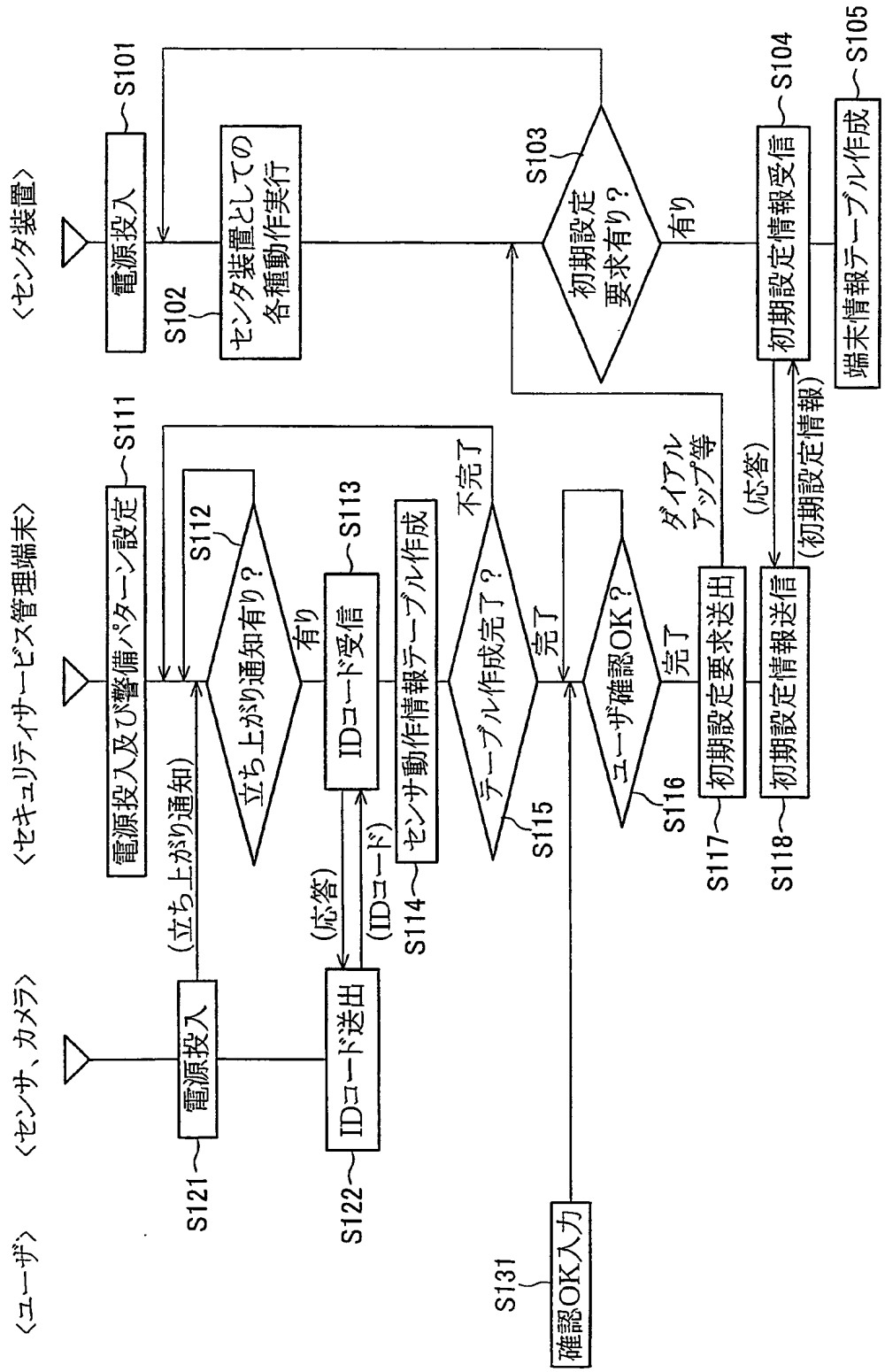

〈ユーザ〉
〈センサ、カメラ〉
〈セキュリティサービス管理端末〉
〈センタ装置〉
電源投入
S101
センタ装置としての各種動作実行
S102
初期設定要求有り？
S103
有り
初期設定情報受信
S104
端末情報テーブル作成
S105
電源投入及び警備パターン設定
S111
立ち上がり通知有り？
S112
有り
IDコード受信
S113
センサ動作情報テーブル作成
S114
テーブル作成完了？
不完了
完了
S115
ユーザ確認OK？
ダイアルアップ等
(応答)
(初期設定情報)
S116
初期設定要求送出
S117
初期設定情報送信
S118
(立ち上がり通知)
電源投入
S121
IDコード送出
S122
(応答)
(IDコード)
確認OK入力
S131

図 9

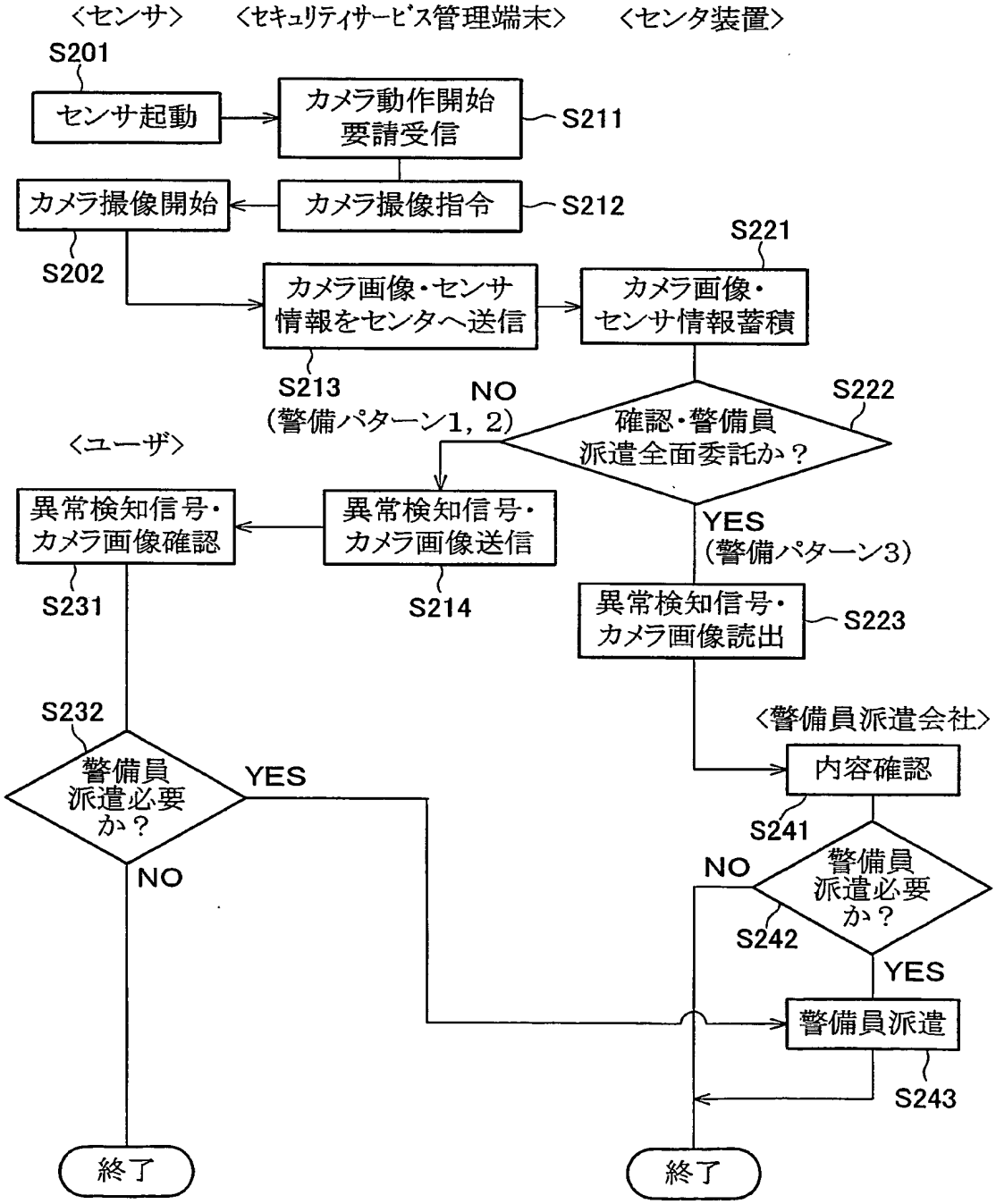

<センサ>
<セキュリティサービス管理端末>
<センタ装置>
S201
センサ起動
カメラ動作開始要請受信
S211
カメラ撮像開始
カメラ撮像指令
S212
S202
S221
カメラ画像・センサ情報をセンタへ送信
カメラ画像・センサ情報蓄積
S213
(警備パターン1, 2)
NO
確認・警備員派遣全面委託か？
S222
<ユーザ>
異常検知信号・カメラ画像確認
異常検知信号・カメラ画像送信
YES
(警備パターン3)
S231
S214
異常検知信号・カメラ画像読出
S223
<警備員派遣会社>
S232
警備員派遣必要か？
YES
内容確認
S241
NO
警備員派遣必要か？
S242
YES
警備員派遣
S243
NO
終了
終了

図 10

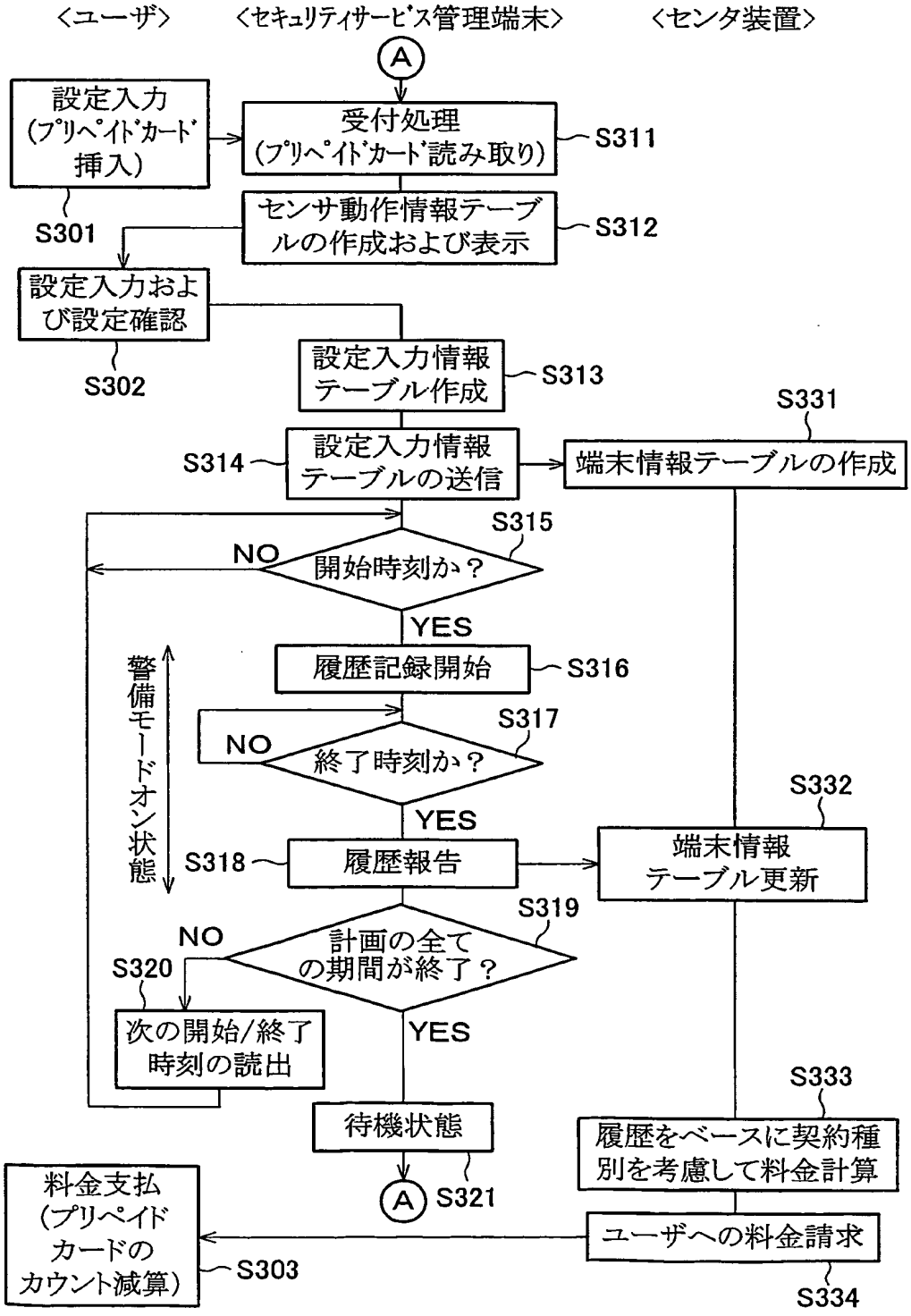

<ユーザ>
<セキュリティサービス管理端末>
<センタ装置>
A
設定入力
(プリペイドカード挿入)
S301
受付処理
(プリペイドカード読み取り)
S311
センサ動作情報テーブルの作成および表示
S312
設定入力および設定確認
S302
設定入力情報テーブル作成
S313
S331
設定入力情報テーブルの送信
S314
端末情報テーブルの作成
S315
NO
開始時刻か？
YES
履歴記録開始
S316
警備モードオン状態
S317
NO
終了時刻か？
YES
S332
履歴報告
S318
端末情報テーブル更新
S319
NO
計画の全ての期間が終了？
S320
次の開始/終了時刻の読出
YES
S333
待機状態
履歴をベースに契約種別を考慮して料金計算
A
S321
料金支払
(プリペイドカードのカウント減算)
S303
ユーザへの料金請求
S334

図 11

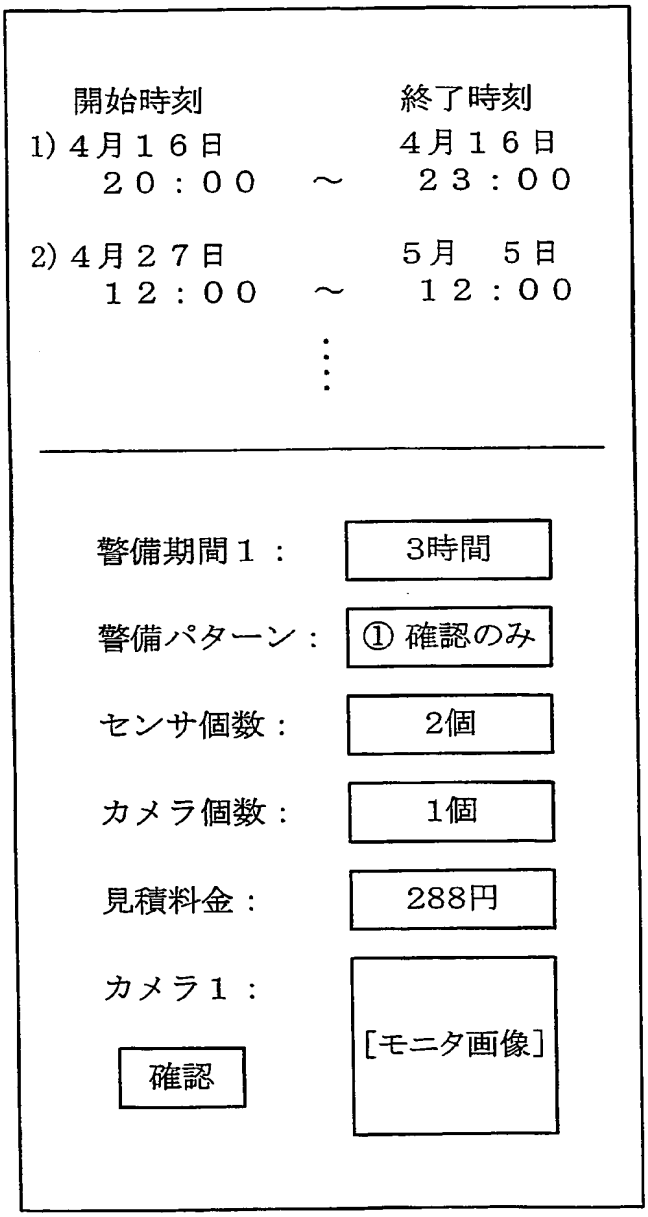

開始時刻
終了時刻
1) ４月１６日
２０：００
～
４月１６日
２３：００
2) ４月２７日
１２：００
～
５月 ５日
１２：００
警備期間１：
3時間
警備パターン：
① 確認のみ
センサ個数：
2個
カメラ個数：
1個
見積料金：
288円
カメラ１：
確認
[モニタ画像]

図 12

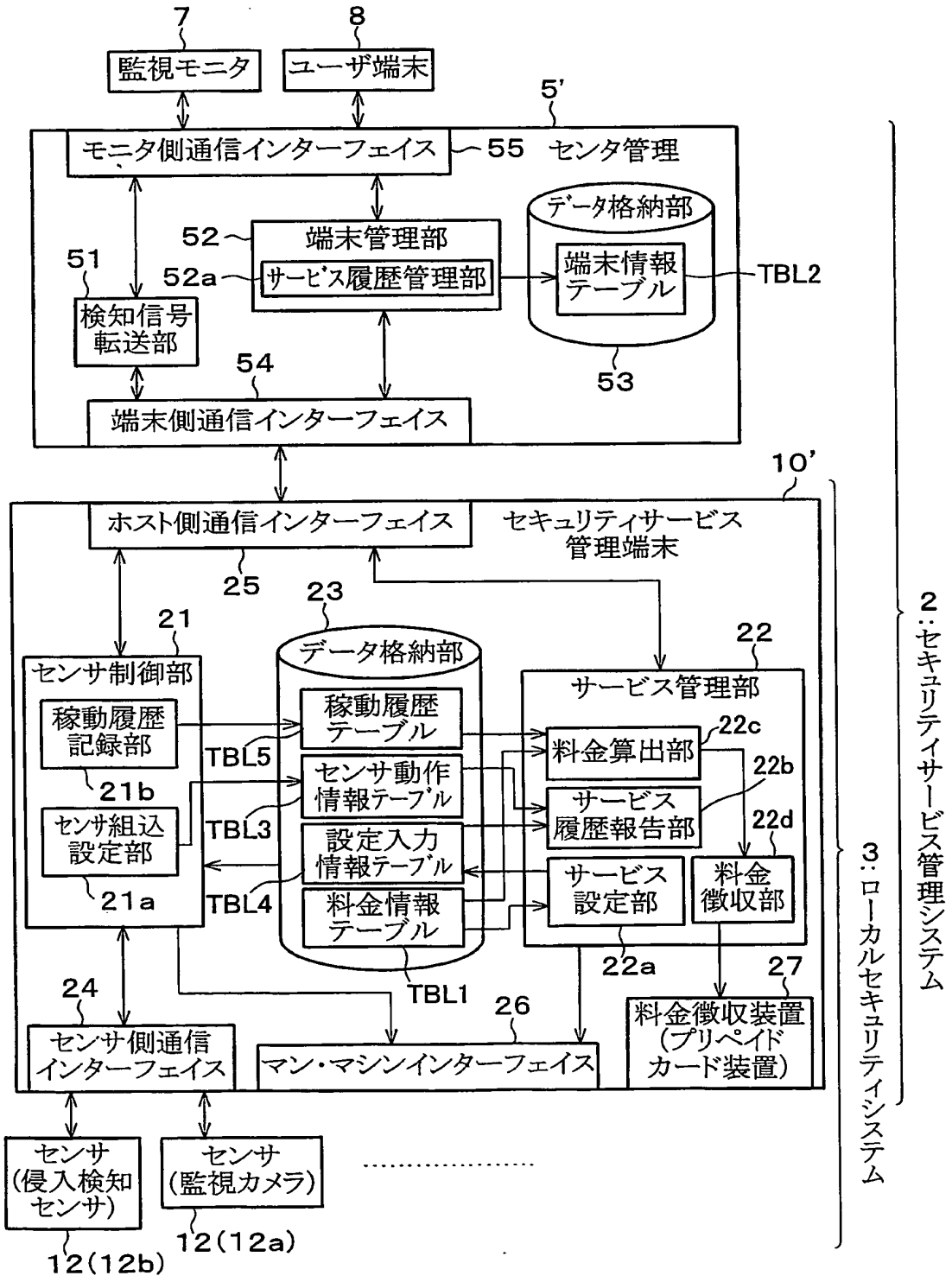
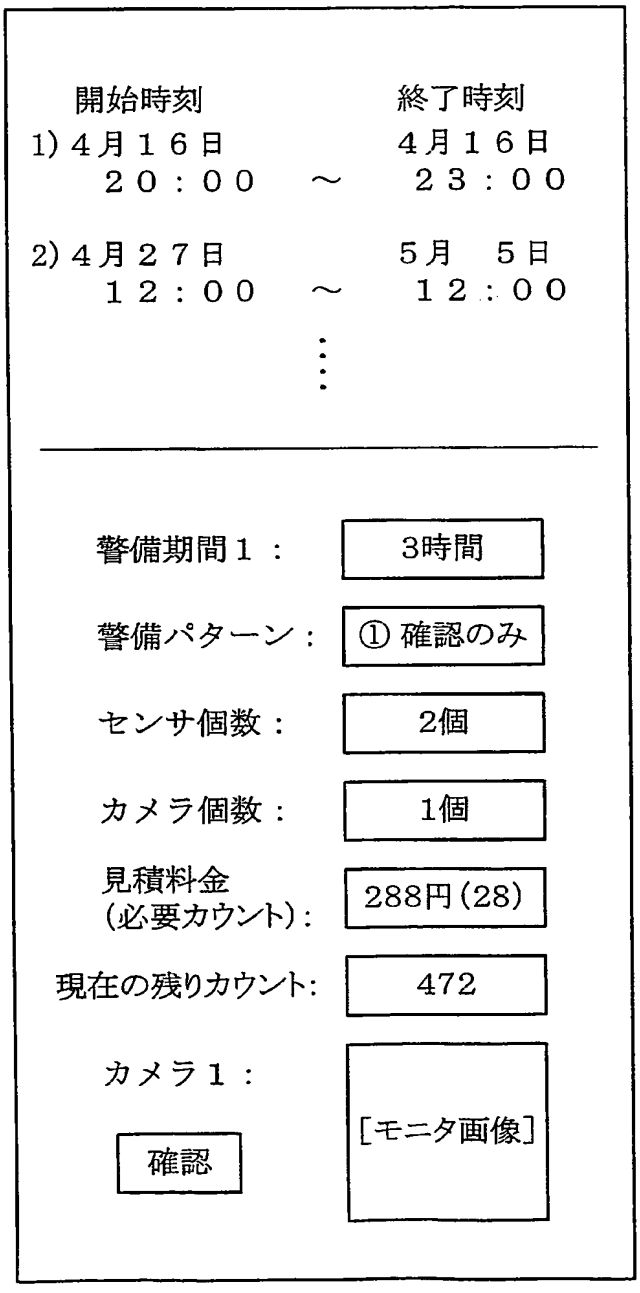

7
8
監視モニタ
ユーザ端末
5'
モニタ側通信インターフェイス
55
センタ管理
データ格納部
52
端末管理部
51
52a
サービス履歴管理部
端末情報テーブル
TBL2
検知信号転送部
54
53
端末側通信インターフェイス
10'
ホスト側通信インターフェイス
セキュリティサービス管理端末
25
23
21
22
センサ制御部
データ格納部
サービス管理部
稼動履歴記録部
稼動履歴テーブル
22c
料金算出部
TBL5
センサ動作情報テーブル
22b
サービス履歴報告部
21b
センサ組込設定部
TBL3
設定入力情報テーブル
22d
サービス設定部
料金徴収部
21a
TBL4
料金情報テーブル
22a
27
24
TBL1
26
料金徴収装置（プリペイドカード装置）
センサ側通信インターフェイス
マン・マシンインターフェイス
センサ（侵入検知センサ）
センサ（監視カメラ）
12(12b)
12(12a)
2：セキュリティサービス管理システム
3：ローカルセキュリティシステム

図 13


開始時刻
終了時刻
1) ４月１６日
２０：００
～
４月１６日
２３：００
2) ４月２７日
１２：００
～
５月 ５日
１２：００
警備期間１：
3時間
警備パターン：
① 確認のみ
センサ個数：
2個
カメラ個数：
1個
見積料金
(必要カウント)：
288円(28)
現在の残りカウント:
472
カメラ１：
確認
[モニタ画像]